Operation/Reference Guide

Modero® CV10

G4 Touch Panels

NXD-CV10 and NXT-CV10

10" Modero Widescreen Video Touch Panels

Touch Panels

Last Revised: 10/10/2007

AMX Limited Warranty and Disclaimer

AMX warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase from AMX, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components that are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX Lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX Lighting products are under warranty. AMX does guarantee the control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality cannot be guaranteed due to the random combinations of dimmers, lamps and ballasts or transformers.
- Unless otherwise specified, OEM and custom products are warranted for a period of one (1) year.
- AMX Software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.

This warranty extends only to products purchased directly from AMX or an Authorized AMX Dealer.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX is not liable for any claim made by a third party or by an AMX Dealer for a third party.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX or an authorized representative of AMX has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY.

FCC Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed an operated with a minimum distance of 20 centimeters between the radiator and your body.

Table of Contents

Introduction 1
CV10 Specifications 3
CV10 Panels - Connector Layout 6
CV10 Touch Panel Accessories 7
NXA-AVB/ETHERNET Breakout Box (FG2254-10) 7
Product Specifications 7
Installing the NXA-AVB/ETHERNET 8
Wiring the NXA-AVB/ETHERNET connectors and cables 9
Wiring the NXA-AVB/ETHERNET for Unbalanced Audio 10
Wiring the NXA-AVB/ETHERNET for Balanced Audio 10
Modero Table Top Cable (CA2250-50) 11
Product Specifications 11
Wiring information for the Modero Table Top cable 12
Installing CAT5 Suppression Ferrites for a CV10 Panel 14
NXA-WC80211B/CF 802.11b Wireless Card (FG2255-03) 16
NXA-WC80211GCF 802.11g Wireless Card (FG2255-07) 17
NXA-CFSP Compact Flash (FG2116-3x) 20
Before Upgrading the Wireless Card - Read This 21
Installation and Upgrade of the Internal NXT Components 21
Step 1: Remove the existing NXT Outer Housing 21
Step 2: Install the Compact Flash Memory card upgrade 22
Step 3: Install the new 802.11g CF Card and Antenna 24
Step 4: Close and Resecure the NXT Panel Enclosure 25
Installation and Upgrade of the Internal NXD Components 26
Step 1: Remove the existing NXD Outer Housing 26
Step 2: Install the new Compact Flash Memory card (NXD) 27
Step 3: Install the new 802.11g Wireless Compact Flash card (NXD) 27
Step 4: Close and Resecure the NXD Panel Enclosure 27
NXT-BP Power Pack (FG2255-10) 28
NXA-BASE/1 Battery Base Kit (FG2255-05K) 28
Checking the NXT-BP charge 29
Installing an NXT-BP into the NXA-BASE/1 30
Installing the NXA-BASE/1 below an NXT-CV10 Panel 30
Charging the NXT-BP using the NXA-BASE/1 31
NXT-CHG Battery Charger Kit (FG2255-50K) 32
Powering the NXT-CHG 33
Reading the NXT-CHG LED Indicator 33

Charging the NXT-BP batteries using the NXT-CHG 33
Recalibrating the batteries 34
Installation 35
Unpacking the Panel 35
Installing the Internal Components 35
Installing the No-Button Trim Ring 35
Installing the Button Trim Ring 37
Pre-Wall Installation of the Conduit Box 38
Installation of an NXD Touch Panel 39
Installing the NXD panel within a Conduit Box 39
Installing the NXD into drywall using Expansion Clips 41
Installing the NXD into a Flat Surface using #4 screws 43
Installing an NXD-CV10 into an (optional) Rack Mount Kit (NXA-RK10) 45
Wiring Guidelines for the CV10 Panels 46
Preparing captive wires 46
Wiring a power connection 46
Audio/Video Port: Connections and Wiring 47
Ethernet/RJ-45 Port: Connections and Wiring 47
USB Port: Connecting and Using Input Devices 48
Panel Calibration 49
Calibrating the Modero Panel 49
Testing your Calibration 50
Configuring Communication 51
Modero Setup and System Connection 51
Configuring and Using USB with a Virtual Master 53
Step 1: Setup the Panel and PC for USB Communication 53
Step 2: Confirm the Installation of the USB Driver on the PC 53
Step 3: Confirm and View the current AMX USB device connections 55
Step 4: Use the USB to Configure a Virtual Master (using NetLinx Studio) 56
Step 5: Confirm and View the current AMX USB device connections 58
Wireless Settings Page - Wireless Access Overview 58
IP Routing 58
Hot Swapping 59
Configuring a Wireless Connection 59
Step 1: Configure the Panel's Wireless IP Settings 60
Wireless communication using a DHCP Address 60
Wireless communication using a Static IP Address 61
Using the Site Survey tool 61
Step 2: Configure the Card's Wireless Security Settings 63

Configuring the Modero's wireless card for unsecured access to a WAP200G 63
Configuring the Modero's wireless card for secured access to a WAP200G 65
Configuring multiple wireless Moderos to communicate to a target WAP200G 69
Configuring a Wired Ethernet Connection 69
Step1: Configure the Panel's Wired IP Settings 69
IP Settings section - Configuring a DHCP Address over Ethernet 70
IP Settings section - Configuring a Static IP Address over Ethernet 70
Step 2: Choose a Master Connection Mode Setting 71
Step 3: Configure an Ethernet Connection Type 71
Master Connection section - Virtual Master communication over Ethernet 72
Master Connection section - NetLinx Master Ethernet IP Address - URL Mode 74
Master Connection section - NetLinx Master Ethernet IP Address - Listen Mode 75
Master Connection section - NetLinx Master Ethernet IP Address - Auto Mode 76
Using G4 Web Control® to Interact with a G4 Panel 76
Using your NetLinx Master to control the G4 panel 78
Upgrading Modero Firmware 81
Upgrading the Modero Firmware via the USB port 81
Step 1: Configure the panel for a USB Connection Type 81
Step 2: Prepare NetLinx Studio for communication via the USB port 82
Step 3: Confirm and Upgrade the firmware via the USB port 83
Upgrading the Modero Firmware via Ethernet (IP Address) 85
Step 1: Prepare the Master for communication via an IP 85
Step 2: Prepare the panel for communication via an IP 86
Step 3: Verify and Upgrade the panel firmware via an IP 87
Firmware Pages and Descriptions 89
Setup Navigation Buttons 89
Setup Page 90
Project Information Page 92
Panel Information Page 93
Time & Date Setup Page 94
Volume Page 96
Supported sampling rates for WAV 97
Protected Setup Page 97
Video Adjustment Page 97
Battery Base Page 98
Protected Setup Navigation Buttons 100
Protected Setup Page 101
G4 Web Control Page 103
Sensor Setup 105

Making the most of the Automated Brightness Control feature (DIM Mode) 107
Password Setup Page 108
Calibration Page 109
Wireless Settings Page 109
Wireless Settings Page - Security Options - Overview 115
Wireless Settings Page - Security Options - Open (Clear Text) 115
Wireless Settings Page - Security Options - Static WEP 116
Wireless Settings Page - Security Options - WPA-PSK 118
Wireless Settings Page - Security Options - EAP-LEAP 119
Wireless Settings Page - Security Options - EAP-FAST 121
EAP Security's Using Server Certificates - Overview 124
Wireless Settings Page - Security Options - EAP-PEAP 124
Wireless Settings Page - Security Options - EAP-TTLS 126
Wireless Settings Page - Security Options - EAP-TLS 129
Client certificate configuration 131
System Settings Page 132
Programming 135
Button Assignments 135
Page Commands 135
Programming Numbers 141
RGB triplets and names for basic 88 colors 141
Font styles and ID numbers 143
Border styles 144
"^" Button Commands 146
Text Effect Names 166
Button Query Commands 167
Panel Runtime Operations 176
Input Commands 180
Embedded codes 181
Panel Setup Commands 182
Dynamic Image Commands 183
Troubleshooting 185
Appendix A 191
Text Formatting Codes for Bargraphs/Joysticks 191
Text Area Input Masking 192
Input mask character types 192
Input mask ranges 193
Input mask next field characters 193
Input mask operations 193

Input mask literals 193
Input mask output examples 194
URL Resources 195
Special escape sequences 195
Appendix B - Wireless Technology 197
Overview of Wireless Technology 197
Terminology 198
EAP Authentication 201
EAP characteristics 201
EAP communication overview 202
AMX Certificate Upload Utility 203
Configuring your G4 Touch Panel for USB Communication 203
Step 1: Setup the Panel and PC for USB Communication 203
Step 2: Confirm the Installation of the USB Driver on the PC 204
How to Upload a Certificate File 205

Introduction

The NXD/T-CV10 10" Modero Widescreen Color Video Touch Panels (FIG. 1) are the industry's first 10-inch widescreen touch panels and are available only through AMX.

NXD-CV10 (front view)
(FG2259-02)

NXT-CV10/PB (front view)
(FG2259-03)

FIG. 1 Sample 10" Video Touch Panels

These Color Video (CV) panels display NTSC/PAL/SECAM video formats within variable sized windows. They include a built-in microphone, speakers, audio/headphone connector, and six NetLinx® programmable pushbuttons (*only available on NXD models with the button feature available (**-02K** and **-03K**)*).

Table Top models use AMX's exclusive **SmoothTilt®** technology for effortless adjustment of the viewing angle.

Each panel is sold only as part of a CV10 Kit which includes both a panel and an NXA-AVB/ETHERNET Audio/Video Breakout Box (**FG2254-10**). This box facilitates the installation and distribution of video (either Composite or S-Video), data (via Ethernet), and audio to Modero touch panels located up to 200 feet (60.96 m) from the breakout box. These panels are ideally suited for displaying full motion video and audio with overlay graphics for applications with demanding visual requirements.

CV10 10" Widescreen Video Touch Panel Kits	
NXD-CV10 (**FG2259-02K**)	10" Widescreen Color Video Wall Mount Touch Panel Kit (with buttons) (includes both an NXD panel and an NXA-AVB/ETHERNET A/V Breakout Box).
NXT-CV10 (**FG2259-01K**)	10" Widescreen Color Video Table Top Touch Panel Kit (without buttons) (includes both an NXT panel with no buttons and an NXA-AVB/ETHERNET A/V Breakout Box).
NXT-CV10/PB (**FG2259-03K**)	10" Widescreen Color Video Table Top Touch Panel Kit (with buttons) (includes both an NXT panel with buttons and an NXA-AVB/ETHERNET A/V Breakout Box).

NOTE

The NXD-CV10 panel (FG2259-02) is shipped, by default with a Trim Ring containing buttons, but the end user can later install the included Trim Ring without button openings.
*NXT panels **can not** be upgraded by simply replacing a Trim Ring on the Faceplate. If you desire an NXT panel with available buttons, you must order the FG2259-03 Kit which includes an NXT panel with buttons (NXT-CV10/PB).*

Key features common to both panels include:

- CV10 panels are based on the latest display technology and support AMX's 4th generation (G4) graphics which provide higher brightness, richer colors, and deeper contrast. The new G4 graphics technology is supported by the latest AMX TPDesign4 Touch Panel Design program.
- CV10 panels display eye-catching images and full-motion video on a large 16:9 image format, while providing a wide 95-degree top-to-bottom viewing angle.
- CV10 panels feature a front panel light sensor, motion sensor, IR receiver and a Sleep/Setup Access combo button.
- CV10 panels are field upgradeable to 802.11g communication via the installation of the new NXA-WC8011GCF Wi-Fi Card Kit (**FG2255-07**).
- CV10 panels support *AMX Computer Control*, which enables remote viewing and control of any networked computer directly from the panel. This gives the user the ability to launch digital music from a PC, cruise the Internet, check and respond to E-mail, open software files, and launch applications. Anything you can do on your PC can be accomplished through these panels.
- The optional wireless solution includes an NXA-WC80211GCF internal Wi-Fi card that allows the CV10 to communicate with a NetLinx Master via a standard 802.11g Wireless Access Point, and an NXA-BASE/1 battery base kit that allows the NXT to function off the charge from the included single NXT-BP battery.
- CV10 panels feature programmable firmware that can be upgraded via either the Ethernet port, wireless interface card, or the mini-USB port.

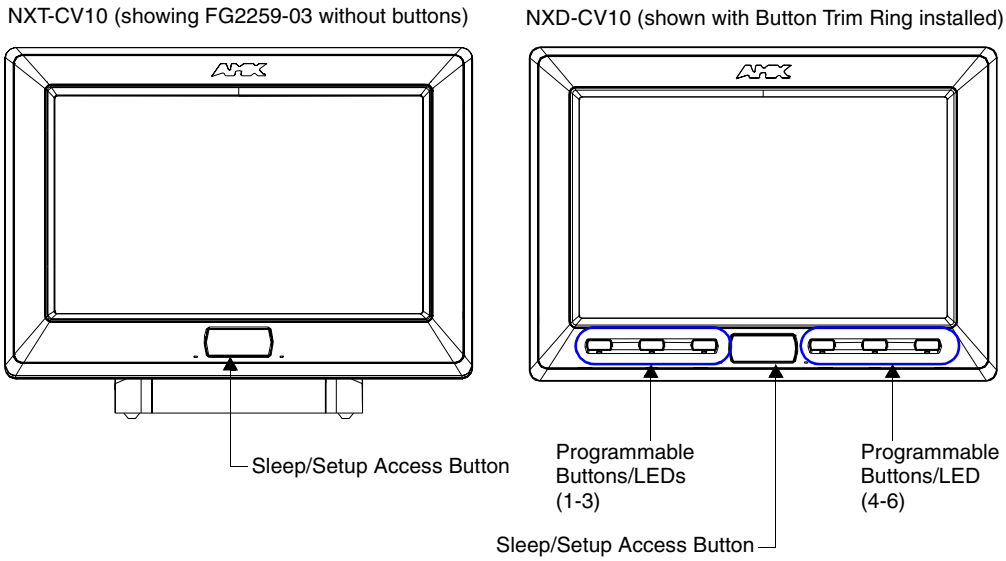

NXT-CV10 (showing FG2259-03 without buttons)
NXD-CV10 (shown with Button Trim Ring installed)
Sleep/Setup Access Button
Programmable Buttons/LEDs (1-3)
Programmable Buttons/LED (4-6)
Sleep/Setup Access Button

FIG. 2 NXT-CV10 and NXD-CV10 (front views)

NOTE

The Button Trim Ring is factory installed only on the FG2259-02 and FG2259-03 panel models.

CV10 Specifications

The following table outlines the specifications for the 10" Widescreen Modero panels.

Specifications for 10" Widescreen Video Touch Panels	
Dimensions (HWD):	• NXA-RK10(*optional*): metal rack-mount with black matte finish: (5 RU - rack units high) 8.72" x 19.0" x 0.50" (22.15 cm x 48.26 cm x 1.27 cm) • NXD-CV10 (with faceplate): 7.96" x 11.16" x 3.32" (20.22 cm x 28.34 cm x 8.43 cm) • NXT-CV10 (Fully raised): 8.71" x 11.16" x 7.38" (22.12 cm x 28.34 cm x 18.75 cm) • NXT-CV10 (Fully lowered): 4.53" x 11.16" x 7.79" (11.51 cm x 28.34 cm x 19.79 cm) • CB-TP10 Conduit/Wallbox (*optional*): 9.23" x 10.90" x 3.40" (23.44 cm x 27.69 cm x 8.64 cm)
Power Requirements (stand-alone CV10):	• Constant current draw: 1.2 A @ 12 VDC (stand-alone) • Startup current draw: 1.2 A @ 12 VDC (stand-alone)
Power Requirements (CV10 and BASE/1):	• Constant current draw: 2.6 A @ 12 VDC • Startup current draw: 3.9 A @ 12 VDC
Memory (factory default):	• 64 MB SDRAM • 64 MB Compact Flash (upgradeable to 1 GB - factory programmed)
Weight (stand-alone):	• NXD-CV10: 2.65 lbs (1.20 kg) • NXT-CV10: 4.75 lbs (2.15 kg)
Certifications:	• FCC Part 15 Class B, CE, and IEC 60950
Panel LCD Parameters:	• Aspect ratio*:* 16 x 9 • Brightness (luminance): 350 cd/m^2 • Channel transparency: 8-bit Alpha blending • Contrast ratio: 250:1 • Display colors: 256 thousand colors (18-bit color depth) • Dot/pixel pitch: 0.28 mm • Panel type: TFT Color Active-Matrix • Screen resolution: 800 x 480 pixels (HV) @ 60 Hz frame frequency • Video format: NTSC, PAL, and SECAM • Viewing angle (95° total viewing angle): Vertical: + 45° (up from center) and - 65° (down from center)
IR Reception Angle:	• Horizontal: ± 50° (left and right from center) • Vertical: ± 30° (up and down from center)
Supported Audio Sample Rates:	• 48000Hz, 44100Hz, 32000Hz, 24000Hz, 22050Hz, 16000Hz, 12000Hz, 11025Hz, and 8000Hz.

Specifications for 10" Widescreen Video Touch Panels (Cont.)	
Front Panel Components:	
Light sensor:	• Photosensitive light detector for automatic adjustment of the panel brightness (a dim room results in a dimmer LCD display, and a bright room results in a brighter LCD display). **Note**: The light sensor can be adjusted via the Sensor Setup page (page 105).
Motion sensor (PIR):	• Proximity Infrared Detector to wake the panel when the panel is approached. • Activation range: ± 45° (left and right from center) and ± 20° (up and down from center). **Note**: This sensor can be adjusted via the Sensor Setup page (see page 105).
IR Receiver:	• IR reception 38 KHz and 455 KHz IR frequencies. • The IR receiver is located beneath the translucent Front Setup button. When an IR code is detected it is sent to the NetLinx Master as a push on the appropriate AMX IR channel. • IR receivers and transmitters on G4 panels share the device address number of the panel.
Front setup access button:	• Provides both access to the Setup and Calibration page and toggles the panel between a "sleep" or "wake" state. - When wired, "sleep" status means the backlight is Off. - When battery operated, wireless "sleep" status means the touch panel base is either Off or "suspended".
Microphone:	• Used for intercom applications (***requires the NXA-AVB/ETHERNET Breakout Box for analog communication***)
Speakers:	• Stereo output with a frequency response of 500 Hz - 7 KHz
LEDs:	• 6 blue LEDs support On and Off (On = *Button pressed*, Off = *Button released*). - ***Both the LEDs and pushbuttons are not available with the NXT-CV10 panel (FG2259-01) containing no buttons.***
Buttons:	• 6 programmable pushbuttons
Rear Panel Components:	(Side panel location on NXD-Wall Mount panels)
Mini-USB connector:	• 5-pin Mini-USB connector used for programming, firmware update, and touch panel file transfer between the PC and the target panel. **Note**: When connecting the panel to PC using a CC-USB (or compatible) cable, be sure to power the panel On before attempting to connect the USB cable from the PC to the mini-USB port on the panel. Refer to the *Configuring and Using USB with a Virtual Master* section on page 53 for more information.
Stereo Output connector:	• Stereo output through a 3.5mm mini-jack (for use with external speakers or headphones).
Ethernet 10/100 port:	• RJ-45 port for 10/100 Mbps communication. The Ethernet port automatically negotiates the connection speed (10 Mbps or 100 Mbps), and whether to use half duplex or full duplex mode. • CV10 panels communicate with the NetLinx Master using the ICSP protocol over Ethernet.
Ethernet 10/100 LEDs:	• LEDs show communication activity and connection information: **A**-activity - Yellow LED lights when receiving or transmitting Ethernet data packets. **L**-link - Green LED lights when the Ethernet cables are connected and terminated correctly.
USB connector:	• Type-A USB port can connect an external keyboard or mouse device for use with Virtual PC applications. **Note**: External USB input devices (keyboard or mouse) must be plugged into the rear/side USB connector **before** the unit is powered-up. The panel will not detect these USB input devices until the unit cycles power.

Specifications for 10" Widescreen Video Touch Panels (Cont.)	
Rear Panel Components (Cont.):	(Side panel location on NXD-Wall Mount panels)
Audio/Video connector:	• RJ-45 connector for communication of differential audio/video signals to/from the touch panel (panel type dependant). This connector receives Composite video, Stereo (left/right) audio, and microphone audio. • Video is received via the NXA-AVB/ETHERNET Breakout Box. Configuring video windows for playback is done using TPDesign4. • In-bound audio (from the breakout box) gets directed to the speakers. • Out-bound audio is sent from the on-board microphone (on the front-panel). Selecting audio files for playback is configured through TPDesign4.
PWR connector:	• 2-pin 3.5 mm mini-Phoenix connector.
Button Assignments (NXD-CV10 only):	Button assignments can only be adjusted in TPD4 and not on the panels. • Button channel range: 1 - 4000 button push and feedback (per address port) • Button variable text range: 1 - 4000 (per address port) • Button states range: 1 - 256 (General Button; 1 = Off State, 2 = On State) • Level range: 1 - 600 (default level value 0-255, can be set up to 1 - 65535) • Address port range: 1 - 100
Operating / Storage Environment:	• Operating Temperature: 0° C (32° F) to 40° C (104° F) • Operating Humidity: 20% - 85% RH • Storage Temperature: -20° C (-4° F) to 60° C (140° F) • Storage Humidity: 5% - 85% RH
Included Accessories:	• Installation Kit for 10" NXD panels (KA2259-02): - 2-pin 3.5 mm mini-Phoenix connector (41-5025) - Four Phillips-head screws (#4-40 x 0.250 Black) - Three Drywall clips (62-5924-05) and #6 - sheet metal screws • Installation Kit for 10" NXT panels (KA2259-01): - 2-pin 3.5 mm mini-Phoenix connector - Cylindrical CAT5 USB Mouse Suppression Ferrite - **One** CAT5 Table Top Suppression Ferrite • Modero Table Top Cable (CA2250-50): provided with all NXT panels. • NXA-AVB/ETHERNET Breakout Box (**FG2254-10**): Provides video/audio distribution to the A/V panel over CAT5 cable (up to 200'/60.96m) and accepts either Composite or S-Video. *- Although the CV10 is only sold as part of a KIT configuration, the breakout box can be purchased as a separate accessory.* • Trim Ring with button openings (60-2259-05) (***factory installed on -02 and -03 panel models only***) • Trim Ring without button openings (60-2259-04) (***NXD models only***)
Other AMX Equipment:	• CB-TP10 (**FG036-10**) - 10" metallic conduit box for Wall Mount installations. • CC-USB (Type A) to Mini-B 5-Wire programming cable (**FG10-5965**) • NXA-BASE/1 Battery Base Kit (**FG2255-05K**) - Battery base and NXT-BP battery (*NXT panels only*) • NXA-RK10 (**FG2904-54**) - RackMount kit for 10" Wall Mount touch panels (***NXD panels only***). Kit includes four #10-32 screws and washers. • NXA-WC80211GCF Wireless Upgrade Kit (**FG2255-07**) - AMX 802.11G Compact Flash provides wireless Ethernet support

Specifications for 10" Widescreen Video Touch Panels (Cont.)	
Other AMX Equipment (Cont.):	• NXT-BP (**FG2255-10**) - Battery pack for Table Top panels. • NXT-CHG Kit (**FG2250-50K**) - Battery charger and 2 NXT-BP batteries • Upgrade Compact Flash (factory programmed with firmware): NXA-CV10CF128M - 128 MB Compact Flash card (**FG2116-65**) NXA-CV10CF256M - 256 MB Compact Flash card (**FG2116-66**) NXA-CV10CF512M - 512 MB Compact Flash card (**FG2116-67**) NXA-CV10CF1G - 1 GB Compact Flash card (**FG2116-68**)

WARNING

It is recommended that firmware KIT files only be transferred over a direct USB or Ethernet connection and only when the panel is connected to a power supply. If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.

CV10 Panels - Connector Layout

FIG. 3 shows the layout of the connectors (located on the rear of the base on the NXT and on the left side panel of the NXD panels).

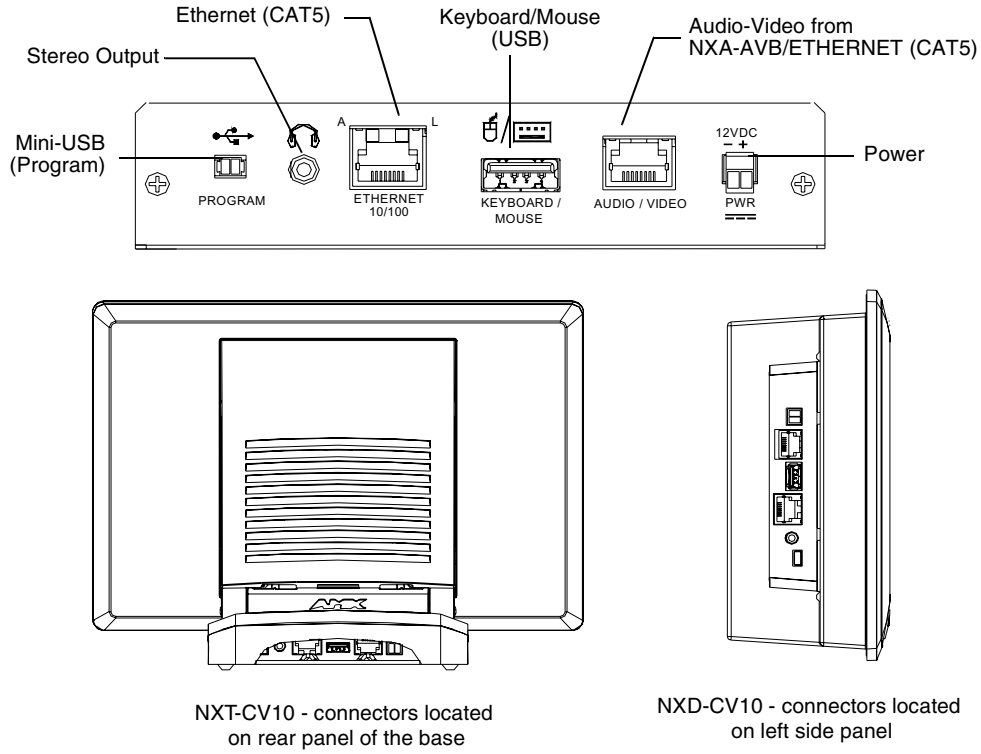


FIG. 3 Connector layout on the CV10 touch panels

CV10 Touch Panel Accessories

The following section outlines and describes both the included accessories and other AMX equipment available for these touch panels.

NXA-AVB/ETHERNET Breakout Box (FG2254-10)

The NXA-AVB/ETHERNET Breakout Box (FIG. 4) is included as part of the CV10 Kit configuration (*panel and box*) but can be purchased as a separate accessory. This box facilitates the installation and distribution of video, data, and audio to Modero touch panels located up to 200 feet (60.96 m) from the AVB box. This unit accepts either Composite or S-Video from standard video devices.

This breakout box can be mounted on either a horizontal flat surface or within an equipment rack (by using an optional AC-RK Rack Kit).

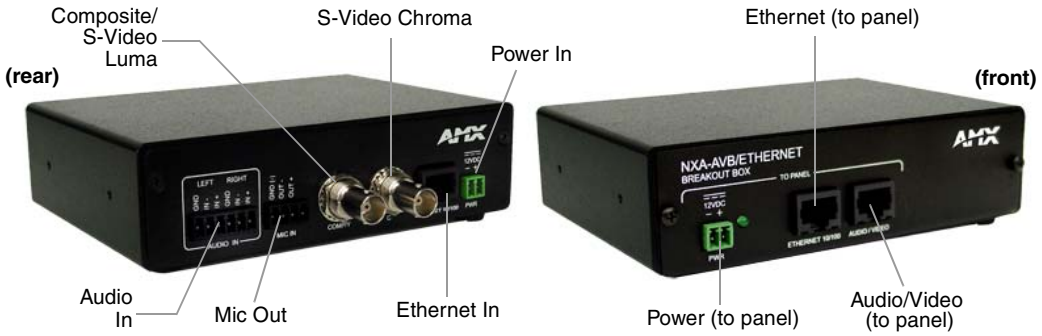


FIG. 4 NXA-AVB/ETHERNET Breakout Box (front and rear views)

Product Specifications

NXA-AVB/ETHERNET Specifications	
Dimensions (HWD):	• 1.50" x 5.55" x 4.88" (3.81 cm x 14.10 cm x 12.40 cm) • Width when attached to mounting ears: 6.65" (16.89 cm)
Power Consumption:	• 50mA (with audio/video input) • 23mA (with no audio/video) • Routed through NXA-AVB/Ethernet using a 12 VDC-compliant power supply
Certifications:	• FCC Part 15 Class B, CE, and EN 60950
Features:	• Accepts either Composite or S-Video (***video-capable panels only***) • Provides audio distribution to the non-video touch panels over a CAT5 cable (up to 200 ft.) • Provides video/audio distribution to the video-capable touch panels over CAT5 cable up to 200 ft. (60.9 m)
Availability:	• This unit is included with CV5, CV7, CV10, and 1200V-Series Kit configurations
Front Components:	• 2-pin 3.5 mm Phoenix connector for power to the touch panel • Green LED provides an indication of power status • RJ-45 connector provides Ethernet signals to the touch panel • RJ-45 connector provides differential audio and video signals to the touch panel (panel type dependant)

NXA-AVB/ETHERNET Specifications (Cont.)	
Rear Components:	• 6-pin 3.5 mm Phoenix connector for in-bound (left/right channel) audio • 4-pin 3.5 mm Phoenix connector for out-bound (from microphone) audio • BNC connector (female) for Composite or Chroma (**for video-capable panels only**) • BNC connector (female) for luminance (**for video-capable panels only**) • RJ-45 connector for Ethernet input from the control system • 2-pin 3.5 mm Phoenix connector for in-bound power
Included Accessories:	• Two 2-pin Phoenix connectors (41-5025) • 4-pin Phoenix connector (41-5047) • 6-pin Phoenix connector (41-5063) • Rack Mount Kit (KA2250-40) with mounting bracket (62-2254-02)
Other AMX Equipment:	• AC-RK Accessory RackMount Kit (**FG515**) • Modero Table Top Cable (CA2250-50)

Installing the NXA-AVB/ETHERNET

A 12 VDC-compliant power supply can indirectly provide power to a Modero panel by routing power through the NXA-AVB/ETHERNET Breakout Box. FIG. 5 shows a sample wiring configuration using both an indirect or direct power connection for a video-capable Modero panel.

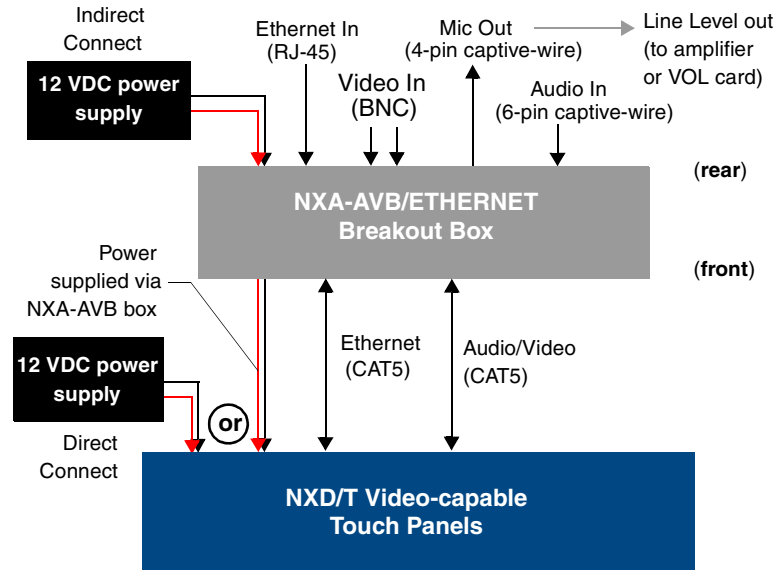


FIG. 5 Sample wiring configuration on video-capable panels using this breakout box

A 12 VDC-compliant power supply can also directly provide power through the unit to a target Modero panel. FIG. 6 shows a sample wiring configuration for a non-video capable Modero panel.

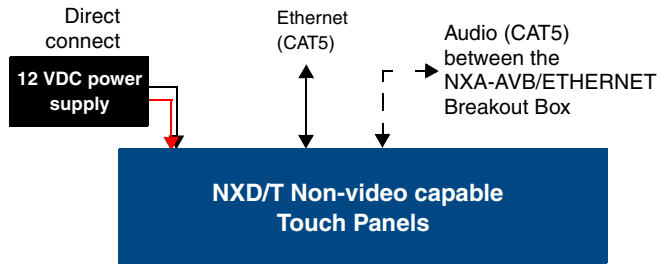

Direct connect
12 VDC power supply
Ethernet (CAT5)
Audio (CAT5) between the NXA-AVB/ETHERNET Breakout Box
NXD/T Non-video capable Touch Panels

FIG. 6 Sample wiring configuration using CA Modero panels

NOTE

The breakout box unit can be mounted on either a horizontal flat surface or into an equipment rack (by removing the front screws and attaching it to an optional AC-RK). The power supply being used on the NXA-AVB/ETHERNET is dependant on the power requirements of the target touch panel.

Use a standard CAT5 Ethernet cable to provide both communication and 10/100 network connectivity between the panel, NXA-AVB/ETHERNET, NetLinx Master, and the network.

Wiring the NXA-AVB/ETHERNET connectors and cables

The inputs and outputs on the breakout box are separated into front and rear connectors. The rear connectors are used to input external signals. The front connectors are used to communicate signals between the NXA-AVB/ETHERNET and a target Modero panel. FIG. 7 provides a layout of the wiring connection both into and from the breakout box.

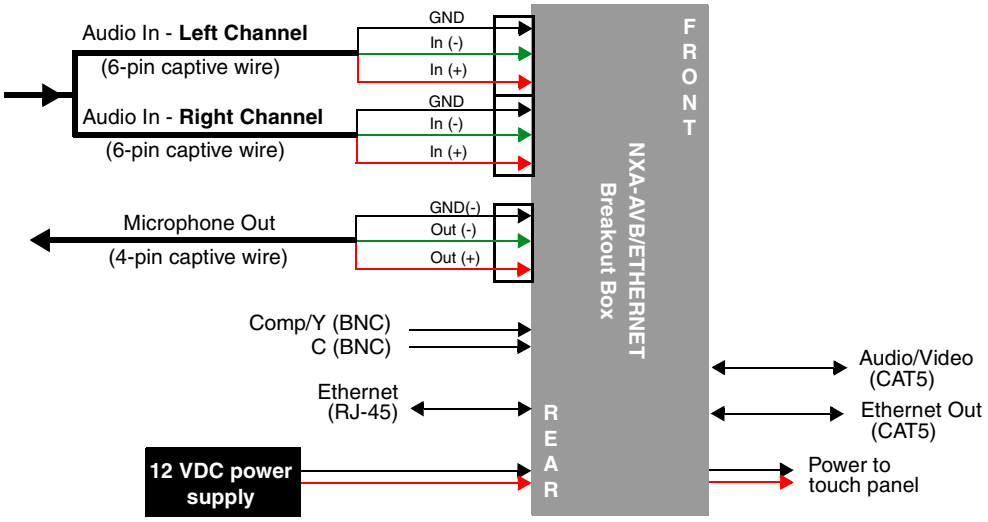


FIG. 7 NXA-AVB/ETHERNET Breakout Box connector wiring diagram

The rear-panel wiring connections are described below (from left to right):

- **AUDIO IN:** 6-pin mini-Phoenix connector, divided into left and right audio channels. Each channel is divided into GND, IN+, and IN- terminal cable connectors (2 sets of 3 for each channel).

  An example of this cable is to strip the ends of 2 RCA audio cables and insert them into their respective locations on the Audio In port.
  Either a balanced (+, -, and GND) or unbalanced (+ and GND) audio signal can be connected to this input.
- **MIC OUT:** 4-pin mini-Phoenix connector, divided into GND, OUT-, and OUT+ terminal connectors.

  An example of this cable is to strip the terminal ends of a 3.5mm mini-jack and insert them into their respective locations on the Mic Out port. This signal can be fed as a Line Level In to either an amplifier or an AMX VOL card.
  Either a balanced (+, -, and GND) or unbalanced (+ and GND) audio signal can be connected to this output.
- **Video In BNCs:** Feeds either Composite/S-Video Luma or S-Video Chroma signals into the NXA-AVB/ETHERNET. This feed is then redirected out to a Modero panel through the front Audio/Video CAT5 port.
- **ETHERNET:** RJ-45 connector routes data to the G4 touch panel through the front Ethernet port. These connections use a standard CAT5 Ethernet cable to provide communication between the target touch panel, breakout box, and NetLinx Master.

- **PWR:** 2-pin mini-Phoenix connector that connects to a 12 VDC-compliant power supply. This port can be used to provide power to a Modero panel by sending it through the NXA-AVB/ETHERNET (rear power connector through to the front power connector).

Wiring the NXA-AVB/ETHERNET for Unbalanced Audio

Most domestic audio equipment has unbalanced audio inputs and outputs. This means that the audio output (left, right, or mono) appears on a single wire, and is referenced to "0 V" or "Ground". Typical connectors used are RCA "phono" connectors, DIN plugs/sockets, and 0.25" (6.3mm) or 3.5mm jack plugs/sockets.

Unbalanced audio is adequate for most domestic environments and for line-level signals in a typical broadcast studio. Problems may occur if the signals are carried over long distances, especially if the source and destination have separate main supplies. Use the following wiring drawing (FIG. 8) to configure an unbalanced audio connection.

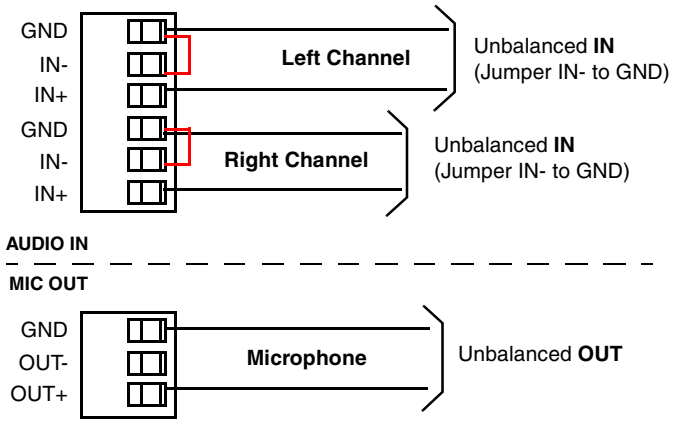


FIG. 8 Wiring the rear AUDIO IN and MIC OUT for use with Unbalanced Audio

When using unbalanced audio for the AUDIO IN connector (FIG. 8), the "-" and the "GND" terminals should be connected together and then connected to the GND of the unbalance audio signal. When connecting to an unbalanced audio input from the MIC OUT connector (FIG. 8), wire the "+" terminal to the signal input, and the "GND" terminal to the signal ground.

Wiring the NXA-AVB/ETHERNET for Balanced Audio

Professional audio equipment will often use balanced audio inputs and outputs, usually on 3-pin "XLR" connectors. A balanced audio signal consists of a pair of wires carrying the audio signal in anti-phase with each other (if one wire carries a positive voltage, the other carries an equal and opposite negative voltage).

The advantage of balanced audio over unbalanced audio is its ability to reject external interference added as the signal is carried over the wire. The receiving equipment takes the voltage difference between the two wires as the input signal. Interference will usually get added to both wires equally, and so gets cancelled by the receiving equipment.

The 3 wires used in a typical XLR lead are often referred to as Ground, Live (Hot) and Return (Cold). "Live" and "Return" carry the "in-phase" and "out-of-phase" versions of the audio respectively. The pins of the XLR plug/socket are as follows:

- X = Ground
- L = Live (Hot)
- R = Return (Cold)

When connecting the MIC OUT connector to a balanced audio input (FIG. 9), use all three audio terminals (+, -, and GND), then connect the "+" terminal to the "live" signal, the "-" terminal to the "return" signal, and the "GND" terminal to the ground signal.

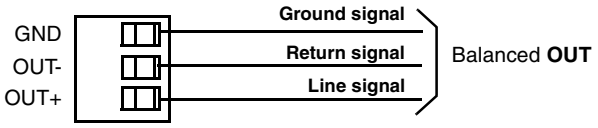


FIG. 9 Wiring the rear MIC OUT connector for use with Balanced Audio

Modero Table Top Cable (CA2250-50)

The Table Top Touch Panel comes with a standard 10' (3.048 m) Modero cable (CA2250-50) that supports Ethernet, Audio/Video, and Power connections. The cable comes terminated with two RJ45 connectors (Ethernet and Audio/Video) and a single 2-pin mini-Phoenix connector for power.

FIG. 10 10 Foot Modero Table Top Cable

Product Specifications

Modero Table Top Cable Specifications	
Dimensions (HWD):	• Length: 10 feet (3.048 m)
Connectors:	• Ethernet RJ-45 connector (White) routes Ethernet signals between the touch panel and the NXA-AVB/ETHERNET Breakout Box. • Audio/Video RJ-45 connector (Black) routes differential audio/video signals between the touch panel and the box. • 2-pin 3.5 mm mini-Phoenix power connector to route power from the external breakout box to the target panel.
Included Accessories:	• Modero Table Top Cable (CA2250-50)

Modero Table Top Cable Specifications (Cont.)	
Other AMX Equipment:	***Note**: All 1200V, VG-Series, and CV10 Table Top panels routing an Audio/Video signal from a breakout box must use the appropriate number of CAT5 Suppression Ferrites which are included as part of installation kits accompanying your particular Modero panel.* Each of the following Installation Kits come with the appropriate number of CAT5 Suppression Ferrites. **These ferrites must be installed onto their appropriate locations.** • Installation Kit for 12" and 17" NXD panels (KA2251-01): - 2-pin mini-Phoenix connector (41-5025) - Three Phillips-head screws (#4-20 x 0.250 Black) (80-0114-08) - **One** CAT5 Suppression Ferrite (04-0014) - Four Drywall clips (62-5924-05) and #6 -metal strips (80-0192) • Installation Kit for 15" NXD panels (KA2251-02): - 2-pin mini-Phoenix connector (41-5025) - Three Phillips-head screws (#4-20 x 0.250 Black) (80-0114-08) - **Two** CAT5 Suppression Ferrites (04-0014) - Four Drywall clips (62-5924-05) and #6 -metal strips (80-0192) • Installation Kit for 12" NXT panels (KA2251-03): - 2-pin mini-Phoenix connector (41-5025) - Three Phillips-head screws (#4-20 x 0.250 Black) (80-0114-08) - **Two** CAT5 Suppression Ferrites (04-0014) • Installation Kit for 15" and 17" NXT panels (KA2251-04): - 2-pin mini-Phoenix connector (41-5025) - Three Phillips-head screws (#4-20 x 0.250 Black) (80-0114-08) - **One** CAT5 Suppression Ferrite (04-0014) • Installation Kit for 10" NXT panels (KA2259-01): - 2-pin 3.5 mm mini-Phoenix connector (41-5025) - **One** CAT5 Table Top Suppression Ferrite (04-0014) - **One** cylindrical CAT5 USB Mouse Suppression Ferrite (04-0018-SA)

Wiring information for the Modero Table Top cable

If your installation requires custom cable configurations, you can purchase bulk (non-terminated) cable from **Liberty Wire and Cable** under the nomenclature *"AMX Table Top Cable - Modero"* (phone#: (800) 530 8998 or +1-719-388-7518). When building a custom Table Top cable, please refer to the table below to calculate the maximum length of the cable for your particular installation/setup.

Maximum Table Top Cable Lengths for Modero Panels					
Panel Sizes:	7" Panel	10" Panel	12" Panel	15" Panel	17" Panel
Setup I: Using a panel *without* a battery base*:					
Maximum cable length	150’ (45.72 m)	150’ (45.72 m)	49’ (14.94 m)	39’ (11.89 m)	10’ (3.05 m)
Setup II: Using a panel *with* a battery base*:					
Maximum cable length	56’ (17.07 m)	56’ (17.07 m)	25’ (7.62 m)	15’ (4.57 m)	10’ (3.05 m)
* The total Modero cable run from the 13.5 V power source.					

* The total Modero cable run from the 13.5 V power source (12 VDC-compliant power supply).

FIG. 11 shows the top and cross-section views of the Table Top cable.

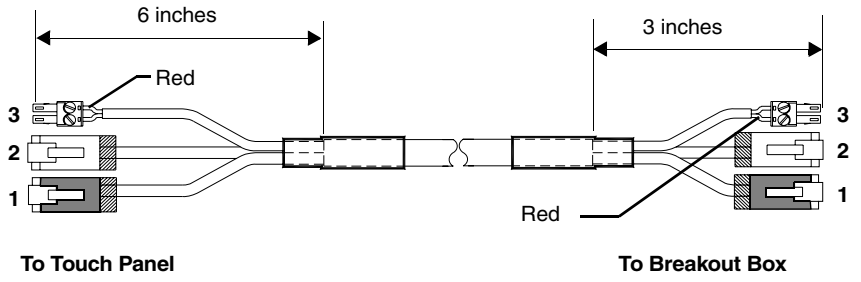


FIG. 11 Modero Table Top cable (top and cross-section views)

The following table provides the wiring information (color coding) for each of the three available cable connectors on each side of the Modero Table Top Cable.

Modero Table Top Cable Wiring Table			
Wire	Connector 1	Connector 2	Connector 3
1	White/Orange	White/Orange	Red
2	Orange/White	Orange/White	Black
3	White/Green	White/Green	-
4	Blue/White	Blue/White	-
5	White/Blue	White/Blue	-
6	Green/White	Green/White	-
7	White/Brown	White/Brown	-
8	Brown/White	Brown/White	-

The following figures provide a cross-section view (FIG. 12) and a description (FIG. 13) of the Modero Table Top Cable:

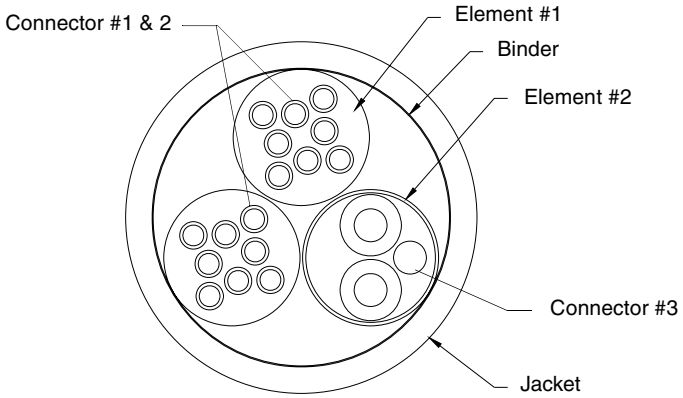


FIG. 12 Table Top Cable - cross-section view

DESCRIPTION:	9/PAIRS COMPOSITE CABLE CONSISTING OF: ELEMENT #1: TWO 4/PAIR 24 AWG STRANDED TINNED COPPER, POLYETHYLENE INSULATION, ELEMENT #2: 1/PAIR 18 AWG STRANDED TNNED COPPER, PVC INSULATION AND FOIL SHIELDED OVERALL PAPER BINDER AND FLEX-PVC JACKET.
ELEMENT #1:	2 X 4/PAIRS: 24 AWG STRANDED COPPER
CONDUCTOR:	24 AWG 7/32 TINNED COPPER; OD .024" NOMINAL
INSULATION:	.0075" WALL POLYETHYLENE; OD .039" NOMINAL
COLOR CODE:	P1: WHITE/BLUE, BLUE P2: WHITE/ORANGE, ORANGE P3: WHITE/GREEN, GREEN P4: WHITE/BROWN, BROWN
PAIR:	2 CONDUCTORS TWINNED LEFT HAND LAY (TWISTED AT VARIED LAYS TO MINIMIZE CROSS TALK)
CABLE:	4/P CABLED LEFT HAND LAY (BLUE BINDER, ORANGE BINDER)
BINDER:	PAPER TAPE
ELEMENT #2:	1 PAIR: 18 AWG SHIELDED
CONDUCTOR:	18 AWG 16/30 TINNED COPPER; OD .046" NOMINAL
INSULATION:	.010" WALL PVC; OD .066" NOMINAL
COLOR CODE:	BLACK, RED
DRAIN WIRE:	#22 7/30 TINNED COPPER
SHIELD:	ALUM/POLYESTER TAPE (FOIL SIDE IN)
FINAL ASSEMBLY:	TWO ELEMENT #1 & ELEMENT #2 CABLED ON COMMON AXIS TO MINIMIZE DIAMETER
BINDER:	CLOTH TAPE 25% OVERLAP
JACKET:	.045" WALL FLEXIBLE PVC,
COLOR:	BLACK MATT
DIAMETER:	.375 INCHES NOMINAL
MARKING:	NONE

FIG. 13 Table Top Cable - Specification Elements

NOTE

Each bundle of 4 twisted pairs includes a colored tape indicator for identification.

Installing CAT5 Suppression Ferrites for a CV10 Panel

Before connecting the RJ-45 cables to the CV10 panel, install the CAT5 Suppression Ferrites (FIG. 14) to their appropriate locations. These ferrites come as part of the Installation Kits mentioned in the previous Specification table. **No tools are required for this installation.**

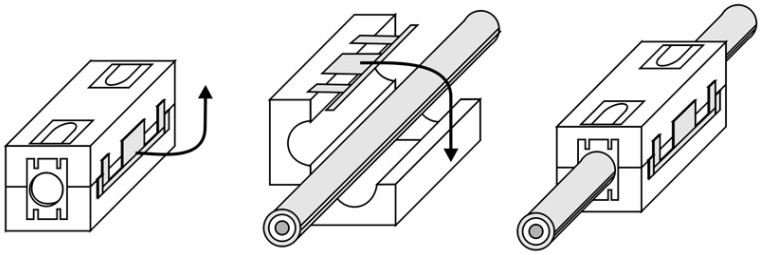

Release the latch to open the plastic enclosure.
Insert the CAT5 cable and close the enclosure.
Push down on the enclosure until it snaps closed.

FIG. 14 Installing the CAT5 Suppression Ferrites

NOTE

All 1200V-Series, VG-Series, and Table Top CV10 panels require the installation of an appropriate number of CAT5 Suppression Ferrites when they use an RJ-45 cable to feed an A/V signal from the breakout box.

1. The CAT5 Suppression Ferrite is housed within a plastic enclosure (shown in FIG. 14) with a latch release on one side. Pull to release the latch and open the enclosure.

2. Grasp the end of the Modero Table Top cable being connected to the panel. This end of the cable is longer than the opposing end which connects to the breakout box (6 inches vs 3 inches). Refer to FIG. 15 for more detailed information.
3. Insert the shrink-wrap section of the cable into the groove along the inside of the ferrite enclosure.

NOTE

The CAT5 Suppression Ferrite MUST be installed onto the shrink-wrap section of the cable, at the location just before the cables split-off and separate.

4. Snap the enclosure shut with the shrink-wrap inside, and proceed to the installation of the second Suppression Ferrite onto the USB mouse cable.
5. Follow these similar procedures to install the additional cylindrical CAT5 USB Mouse Suppression Ferrite (04-0018-SA):
   - Locate the USB mouse device that will be connected to the rear USB connector on the NXT panel.
   - Choose a location on the cable (*closest to the connection point on the touch panel*) and insert it into the groove along the inside of the cylindrical enclosure.
   - Snap the enclosure shut with the USB cable inside, and you're done.

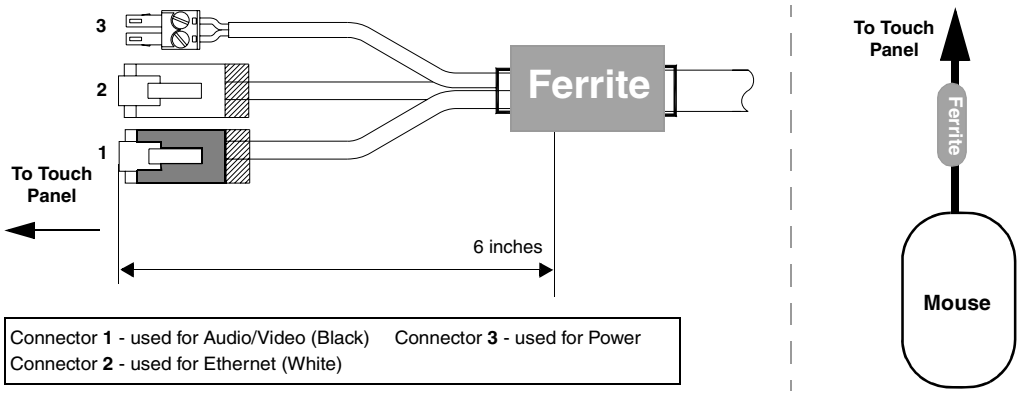


FIG. 15 CV10 Ferrite connector location on the Table Top and mouse cables

NXA-WC80211B/CF 802.11b Wireless Card (FG2255-03)

These touch panels can connect to a wireless network using an optional AMX 802.11b Wireless Interface Card shown in FIG. 16. This internal card is field-upgradeable within both models of panels.

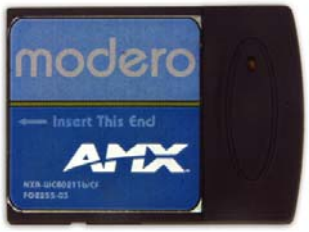


FIG. 16 NXA-WC80211B/CF Wireless Interface Card (WIC)

NOTE

This unit is certified and available for use in the United States (FCC), Canada (IC), Europe (CE) and Japan (TELEC).

The NXA-WC80211B/CF Wireless Interface Card works with compatible 802.11b Wireless Access Points such as the NXA-WAP200G. Please follow your particular Wireless Access Point's instruction manual for the correct procedures to setup either a secured or unsecured connection.

802.11b Wireless Interface Card Specifications	
Dimensions (HWD):	• 2.07" x 1.68" x 0.21" (52.56 mm x 42.80 mm x 5.57 mm)
Weight:	• 13.61 grams (0.030 lbs)
Description:	• 2.4 GHz Direct Sequence Spread Spectrum (DSSS) 802.11b 11M wireless PC card with detachable Antenna.
Features:	• Wired Equivalent Privacy (WEP) 64-bit and 128-bit data encryption • Diversity Antenna Connectors automatically select the best available signal • Supports infrastructure (communications to wired networks via Access Points), and roaming (standard IEEE 802.11b compliant)
Antenna:	• 2, Ceramic (Diversity Supported)
Certifications:	• FCC (United States) • IC (Canada) • CE (Europe) • TELEC (Japan)
Host Interface:	• Compact Flash Type I
Interoperability:	• Interoperable with Wi-Fi (WECA) certified products
LED Indicators:	• Power / Link activity
Modulation:	• DSSS, DBSK, DQSK, CCK
Network Standard:	• IEEE 802.11b
Number of Channels:	• 14
Operating Voltage:	• 5 / 3.3 V

802.11b Wireless Interface Card Specifications (Cont.)	
Operating Channels:	• 11 Channels (USA, Canada) • 13 Channels (Europe) • 14 Channels (Japan) • 4 Channels (France)
Operating Environment:	• Temperature: 0°C ~ 70°C (non-operating) and -15 ~ 80°C (storage) • Humidity (non-condensing): 5% ~ 95% RH
Power Consumption:	• TX power consumption: ≤ 265 mA • RX power consumption: ≤ 165 mA • Sleep Mode: 2 mA - 15 mA
Radio Data Rate:	• 1Mbps, 2Mbps, 5.5Mbps, 11Mbps, Auto Rate
Receive Sensitivity:	• @PER < 8% 11 Mbps: -83 dBm (max) 5.5 Mbps: -86 dBm (max) 2 Mbps: -89 dBm (max) 1 Mbps: -92 dBm (max)
RF Output Power:	• 15 dBm +/- 1 dBm • Channels 1 - 11 (North America)
Security:	• WEP 64,128 bit, WPA/TKIP
Wireless Restrictions:	• In R&TTE countries, such as France, the 802.11g frequency band is restricted to 2454 - 2483.5 MHz (2.4 - 2.4835 GHz) and a max power output of 100 mW EIRP outdoor.

NOTE

It is recommended that any upgrade of internal equipment be done simultaneously in order to reduce the risk of damage to internal components.

NXA-WC80211GCF 802.11g Wireless Card (FG2255-07)

These panels can also connect to a wireless network using the (optional) 802.11g Wi-Fi CF card. This internal WIC (FIG. 17) can be purchased separately as a Wi-Fi upgrade kit from AMX.

FIG. 17 NXA-WC80211GCF 802.11g wireless card

This interface card (**FG2255-07**) is a 2.4 GHz Wi-Fi LAN CF Card which upgrades a Modero panel's wireless RF capabilities from 802.11b to 802.11g. This card also provides the end-user with several new methods of wireless encryption and data security such as WPA and WPA2. In addition to being backwards compatible with 802.11b networks, this card is installable within all current MVP, CV7, and CV10 panels. To fully utilize these newer wireless security features, this card must be used in tandem with the latest Modero firmware upgrade available at **www.amx.com**.

This card works with compatible 802.11b/g Wireless Access Points such as the NXA-WAP200G (*which uses a default SSID of **AMX***). Please follow your particular Wireless Access Point's instruction manual for the correct procedures to setup either a secured or unsecured connection. The following table lists the specifications for the NXA-WC80211GCF.

This upgrade kit requires that pre-existing panels first be removed from their current location (surface, wall or docking station) before an installer can access the internal circuit boards and upgrade a pre-existing 802.11b wireless CF card.

Only MVP panels require the use of a cardboard cutout (Mounting Template) to properly position the metal antenna plate onto the inner surface of the unit's rear plastic housing

CV7 and CV10 panels only require locating the Compact Flash's metal cover plate on the main circuit board and then adhering the terminal antenna connector to that location using the included double-sided adhesive tape.

If the CF metal cover plate is not present over the wireless card slot on a CV7 or CV10 panel, you can use the adhesive tape to secure the terminal antenna to the surface of the new card (atop the product label).

The procedures for upgrading a CF card on an MVP is identical for both MVP-7500 and MVP-8400 panels. The procedures for upgrading/installing the new CF card are also similar across all referenced NXT panels and NXD panels as a group (differences arise from their housing).

NXA-WC80211GCF Specifications	
Dimensions (HWD):	• 0.22" x 1.68" x 2.40" (5.6 mm x 42.80 mm x 61.0 mm)
Weight:	• 19.50 grams (0.043 lbs)
Description:	• Wireless LAN Compact Flash Card with external PIFA antenna. • Features enterprise-class security such as WPA and WPA2 security.
Features:	• Compact Flash Type I form factor • Enhanced range and throughput • Features wireless security such as: WPA, WPA2 and WEP • Field-installable • Incorporates DSSS and OFDM radio technology • Operates at ISM frequency bands of 2.4 GHz, while providing data transfer speeds of up to 54Mbps. • Support for IEEE 802.11b and 802.11g • Supports Advanced Encryption Standard (AES) 64-bit and 128-bit data encryption, along with an Re4 encryption cipher (64/128-bit) • Supports authentication methods such as: EAP-FAST, EAP-LEAP, EAP-PEAP, EAP-TLS, and EAP-TTLS • Supports Wired Equivalent Privacy (WEP) 64-bit and 128-bit data encryption (known to the on-board firmware as Static WEP)
Antenna Type:	• External PIFA antenna (factory-installed)
Bus Interface:	• Compact Flash Type I
Certifications:	• FCC Part 15 Class B, CE, IC, TELEC, and Wi-Fi
Media Access Control Techniques:	• Using 802.11b DSSS communication: DBPSK @ 1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 Mbps • Using 802.11g OFDM communication: BPSK @ 6 and 9 Mbps QPSK @ 12 and 18 Mbps 16-QAM @ 24 and 36 Mbps 64-QAM @ 48 and 54 Mbps

NXA-WC80211GCF Specifications (Cont.)	
Network Architecture:	• Infrastructure mode (Client-to-Access Point)
Operating Channels:	• Using 802.11b & g communication: - 04: (Ch 10 - 13) - France - 11: (Ch 1 - 11) - North America - 13: (Ch 1 - 13) - Europe ETSI - 13: (Ch 1 - 13) - Japan (802.11g) - 14: (Ch 1 - 14) - Japan (802.11b) **Note**: **To alter the card's default country code (North America), please contact an AMX Technical Support representative for detailed procedures and information.**
Operating Environment:	• Temperature: 0°C ~ 45°C (32°F to 113°F) (operating) and -20°C ~ 70°C (-4°F to 158°F) (storage) • Humidity: (non-condensing) 5% ~ 90% RH (operating) and (non-condensing) 5% ~ 95% RH (storage)
Operating Voltage:	• 3.3V + 5% I/O supply voltage
Power Consumption:	• @ 802.11b communication: - RX: 270 mA - TX: 435 mA - Standby: 240 mA • @ 802.11g communication: - RX: 270 mA - TX: 460 mA - Standby: 240 mA
Radio Data Rate:	• 802.11g compliant: 1, 2, 5.5, 11 (DSSS/CCK); 6, 9, 12, 18, 24, 36, 48, and 54 (OFDM) Mbps data rates
Radio Technology:	• Using 802.11b communication: DSSS (Direct Sequence Spread Spectrum)/CCK (Complementary Code Keying) • Using 802.11g communication: DSSS/CCK, OFDM (Orthogonal Frequency Division Multiplexing
Receiver Sensitivity:	• Using 802.11b communication @ FER<8%: 1 Mbps: -94 dBm (max) 2 Mbps: -93 dBm (max) 5.5 Mbps: -92 dBm (max) 11 Mbps: -90 dBm (max) • Using 802.11g communication @ PER <10%: 6 Mbps: -87 dBm (max) 9 Mbps: -86 dBm (max) 12 Mbps: -86 dBm (max) 18 Mbps: -84 dBm (max) 24 Mbps: -82 dBm (max) 36 Mbps: -78 dBm (max) 48 Mbps: -74 dBm (max) 54 Mbps: -72 dBm (max)
RF Frequency Ranges:	• Using 802.11b & g communication: Europe ETSI: 2.412 ~ 2.472 GHz France: 2.457 ~ 2.472 GHz Japan (802.11b): 2.412 ~ 2.484 GHz Japan (802.11g): 2.412 ~ 2.472 GHz North America: 2.412 ~ 2.462 GHz
Standard Conformance:	• IEEE 802.11b • IEEE 802.11g • IEEE 802.11e • IEEE 802.11i • Wi-Fi (WPA and WPA2)

NXA-WC80211GCF Specifications (Cont.)	
Transmit Output Power:	• 802.11b communication: 12 +-1 dBm (1, 2, 5.5, 11 Mbps) • 802.11g communication: 12 +-1 dBm (6, 9, 12, 18, 24, 36, 48, and 54 Mbps)
Wireless LAN Security:	• EAP-FAST • EAP-LEAP • EAP-PEAP • EAP-TLS • EAP-TTLS • WEP 64 & 128 • WPA-PSK
Touch Panel Compatibility:	• MVP-7500 (**FG5965-01**) • MVP-8400 (**FG5965-02**) • NXD-CV10 (**FG2259-02**) • NXT-CV10 (**FG2259-01/03**) • NXD-CV7 (**FG2258-02**) • NXT-CV7 (**FG2258-01**)
Included Accessories:	• Double-sided adhesive tape • Mounting Template cutout (62-2255-04) • NXA-WC80211GCF Installation Guide • Two Alcohol cleaning pads • Wireless CF card with wireless antenna
Other AMX Equipment:	• NXA-WAP250G Modero Wireless Access Point (**FG2255-50**) • Upgrade Compact Flash memory (factory programmed with firmware): NXA-CFSP128M - 128 MB compact flash card (**FG2116-36**) NXA-CFSP256M - 256 MB compact flash card (**FG2116-37**) NXA-CFSP512M - 512 MB compact flash card (**FG2116-38**) NXA-CFSP1GB - 1 GB compact flash card (**FG2116-39**)

NXA-CFSP Compact Flash (FG2116-3x)

Every CV10 Modero panel is shipped with a 64 MB Compact Flash card (NXA-CFSP).

NOTE

If possible, upgrade the panel's internal components (Compact Flash or wireless interface cards) prior to installing or using the panel.

The NXA-CFSP Compact Flash card is factory programmed with specific panel firmware and can be upgraded to several sizes, up to 1GB:

Optional Compact Flash Upgrades	
• NXA-CV10CF128M - 128 MB Compact Flash card	(**FG2116-65**)
• NXA-CV10CF256M - 256 MB Compact Flash card	(**FG2116-66**)
• NXA-CV10CF512M - 512 MB Compact Flash card	(**FG2116-67**)
• NXA-CV10CF1G - 1 GB Compact Flash card	(**FG2116-68**)

Upgrading the Compact Flash card in both panel types involves opening the panel enclosure/outer housing to access the internal circuit board, removing the existing card, replacing it with the 802.11g upgrade, and then resecuring the panel enclosure, as described in the following sections.

Before Upgrading the Wireless Card - Read This..

NOTE

This new firmware file provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.

1. Upload the latest **panel-specific kit file** to your existing Modero touch panel and then confirm the firmware file update was successful.

CAUTION

If you don't first update the firmware file on the panel, before proceeding with the card upgrade process, you will be required to configure NetLinx Studio to communicate with the target panel via a direct USB connection.
In this communication scenario, your PC acts as a Virtual NetLinx Master establishing a secure USB connection to the target panel and then uploading the new Kit file.

Installation and Upgrade of the Internal NXT Components

Upgrading the cards within the Table Top panel involves removing the outer housing (with speaker plate), removing the existing card, replacing it with the 802.11g upgrade, and then placing the outer housing back onto the NXT panel, as described in the following sections.

These panels do not come factory installed with the NXA-WC802.11GCF wireless interface card. This card must be ordered separately from AMX as part of the 802.11g upgrade kit (**FG2255-07**).

NOTE

***Do not** use Ethernet cables containing mounting boots. These boots could make removal of the Ethernet connectors (from the panel) difficult and cumbersome.*

Step 1: Remove the existing NXT Outer Housing

1. Carefully detach all connectors from the rear of the touch panel and then gently place the touch panel LCD facedown onto a soft cloth to expose the under-side of the base (FIG. 18). This step helps prevent scratching of the LCD.
2. Tilt the base forward so that both the bottom surface and Housing Screws are easily accessible.

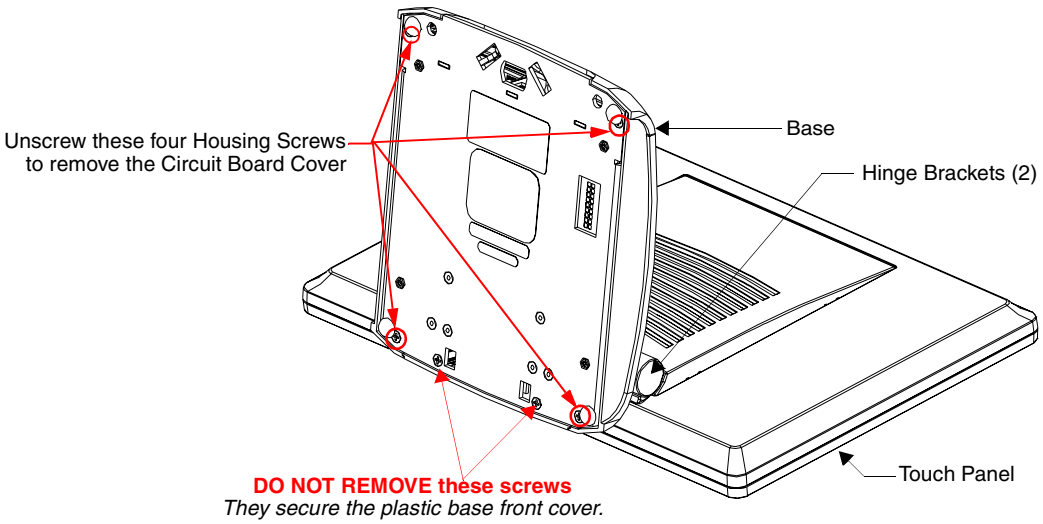

Unscrew these four Housing Screws
to remove the Circuit Board Cover
Base
Hinge Brackets (2)
Touch Panel
DO NOT REMOVE these screws
They secure the plastic base front cover.

FIG. 18 Location of the attachment screws underneath an NXT-CV10 panel base

3. While holding the outer housing and base plate at an angle (*to prevent it from sliding*), use a grounded Phillips-head screwdriver to remove the four Housing Screws.

NOTE

Note the location of the four plastic adhesive "feet". Once the outer housing is placed back onto the panel, these "feet" must be placed back onto their original locations so they can fit into their provided openings on a Battery Base.

4. Rotate the panel back over (while gripping the entire unit and outer housing) and rest the base back onto a flat surface.
5. Gently tilt the LCD panel backwards to expose the Tilt Bracket/Speaker assembly (FIG. 19).

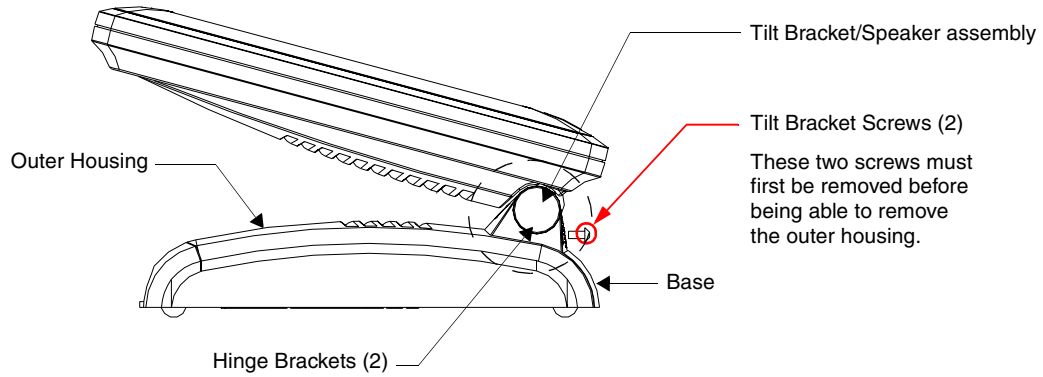

Tilt Bracket/Speaker assembly
Tilt Bracket Screws (2)
These two screws must first be removed before being able to remove the outer housing.
Outer Housing
Base
Hinge Brackets (2)

FIG. 19 Location of the Tilt Bracket screws

6. Locate the two screw holes at either sides of the front speaker grill and then use a grounded Phillips-head screwdriver to remove the two Tilt Bracket Screws (FIG. 19). This procedure both loosens the rear Tilt Bracket cover plate (*with the AMX logo and Hinge brackets*) and provides greater flexibility for the removal of the outer housing. ***Without this step, the Hinge brackets (FIG. 19) present an obstacle to the removal of the outer housing and restrict access to the circuit board.***
7. Tilt the LCD panel back up to gain better access to the Tilt Bracket cover plate.
8. *In a single motion*, carefully pull both the Tilt Bracket cover plate and outer housing up and then out (away from the LCD panel) to expose the internal circuit board (FIG. 20).

Step 2: Install the Compact Flash Memory card upgrade

1. Discharge any static electricity from your body by touching a grounded metal object and then locate the existing 64 MB Compact Flash card on the main board (FIG. 21).
2. Insert the tip of a grounded flat-head screwdriver into one of the card removal grooves (located on either side of the existing card), and gently pry the card out of the slot (FIG. 22). Repeat this process on the opposite card removal groove. This alternating action causes the card to "wiggle" away from the on-board connector pins.
3. Grip the old card by its sides and then carefully pull it out of the slot.

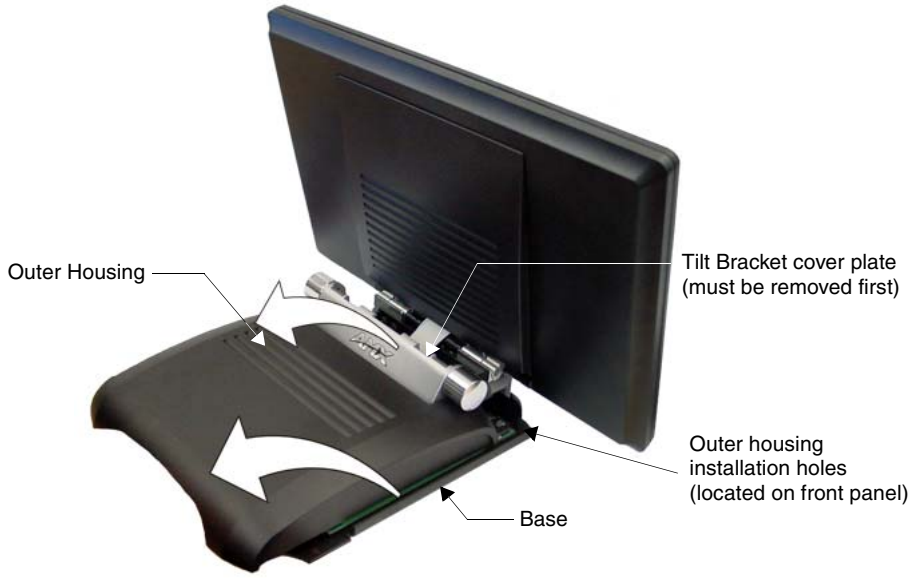


FIG. 20 Removal of the outer housing and wireless card location

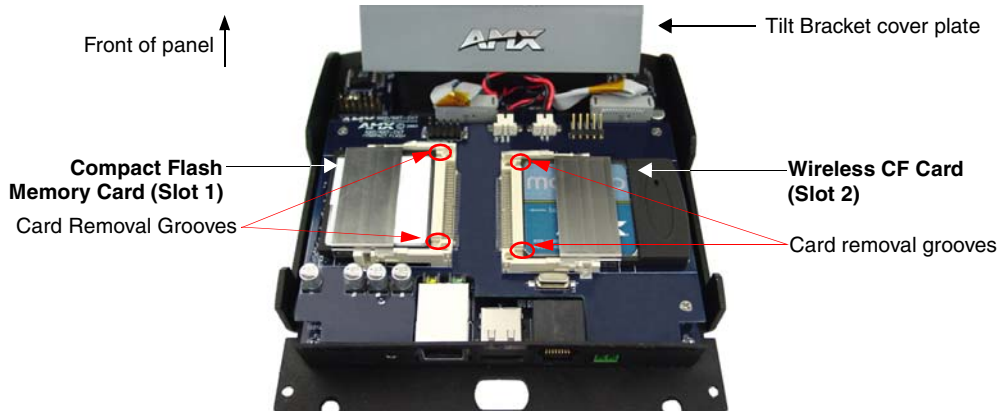


FIG. 21 Location and orientation of the card slots (both CV10 panels)

4. Remove the new CF memory card from it's anti-static bag.
5. Firmly grip the sides of the new CF memory card and insert it firmly into slot opening (with the arrow facing towards the pins) until the contact pins are completely inside the flash card and it is then securely attached to the pin sockets.
6. To complete the upgrade process, either upgrade the remaining wireless card (Step 3) or close and re-secure the enclosure using the procedures in *Step 4: Close and Resecure the NXT Panel Enclosure* section on page 25.

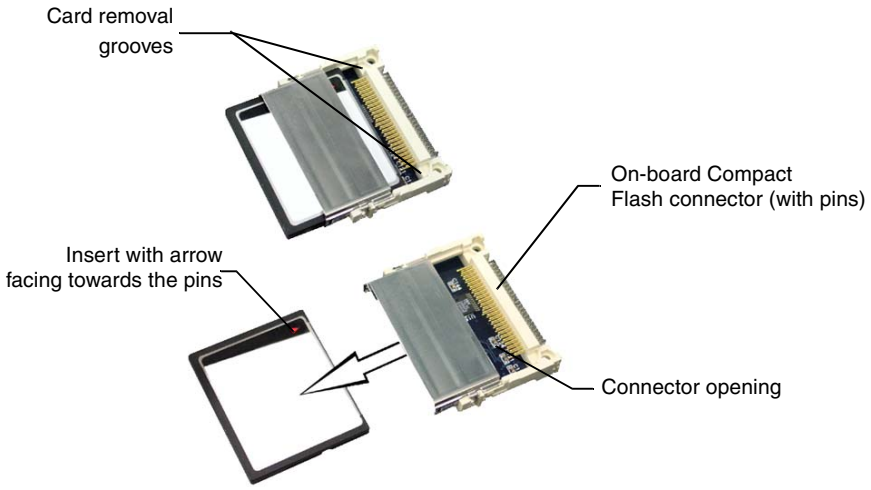

Card removal grooves
On-board Compact Flash connector (with pins)
Insert with arrow facing towards the pins
Connector opening

FIG. 22 Removing/installing a Compact Flash Memory card

NOTE

Any new internal card upgrade is detected by the panel only after power is cycled.

Step 3: Install the new 802.11g CF Card and Antenna

1. Discharge any static electricity from your body by touching a grounded metal object and then locate the wireless card slot on the main board (FIG. 23).
2. Insert the tip of a grounded flat-head screwdriver into one of the card removal grooves (located on either side of the existing card), and gently pry the card out of the slot (FIG. 23). Repeat this process on the opposite card removal groove. *This alternating action causes the card to "wiggle" away from the on-board connector pins.*
3. Grip the old card by its sides and then carefully pull it out of the slot.
4. Remove one of the included alcohol pads and use it to thoroughly clean both the CF metal cover (FIG. 23) and the metal pate on the underside of the terminal antenna. These surfaces must be properly cleaned to provide good adhesion for the later installation of the wireless antenna.

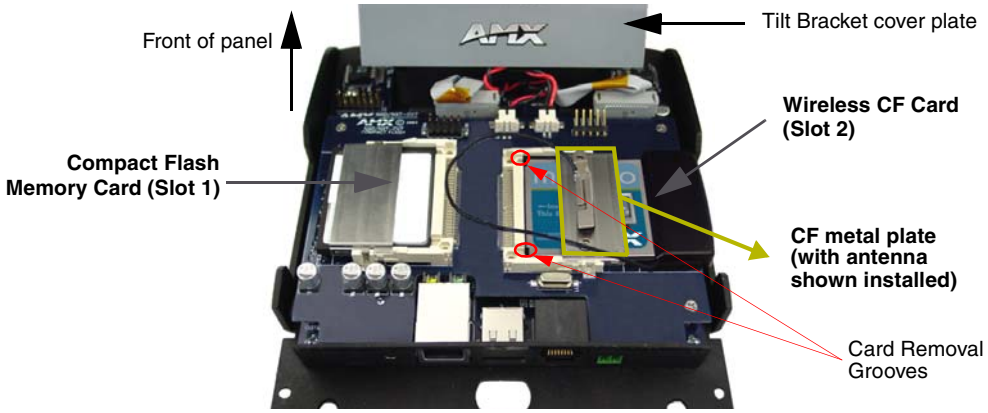

Front of panel
Tilt Bracket cover plate
Wireless CF Card (Slot 2)
Compact Flash Memory Card (Slot 1)
CF metal plate (with antenna shown installed)
Card Removal Grooves

FIG. 23 Location and orientation of the card slots (both CV7/CV10 panels)

5. Remove the new NXA-WC80211G CF card from it's anti-static bag.
6. Grip the sides of the new wireless card and insert it firmly into the slot opening until the contact pins are completely inside the card and securely attached to the pin sockets.

NOTE

You must precisely align the double-sided tape to the surface of the antenna's metal plate in order to properly secure the antenna within to the CF metal cover plate.

7. Carefully peel-off one side of the included double-sided tape and adhere the adhesive side to the surface of the antenna's metal plate.
8. Grip the antenna by its sides and carefully peel-off the remaining protective film on the double-sided tape.
9. Align the antenna atop the CF metal cover plate and press down firmly to securely adhere it.

NOTE

If the CF metal cover plate is not present over the wireless card slot, you can use the adhesive tape to secure the terminal antenna to the surface of the new card (atop the product label).

10. To complete the upgrade process, close and resecure the panel enclosure using the procedures in the following step.

Step 4: Close and Resecure the NXT Panel Enclosure

1. ***In a single motion***, gently slide the rear Tilt Bracket cover plate back over the tilt mechanism (*located below the LCD*) and (*while angling the housing downwards*) slide the outer housing below the Tilt Bracket and towards the LCD (at a downward angle).
2. Locate the two screw holes at either sides of the front speaker grill and then use a grounded Phillips-head screwdriver to both insert and secure the two Tilt Bracket Screws (FIG. 19). This procedure resecures the rear Tilt Bracket cover plate (*with the AMX logo and Hinge brackets*).
3. Press the outer housing forwards until it is aligned over the outer housing installation holes. Once installed and secured, the tilt bracket prevents any further movement (FIG. 20).
4. Gently press down on the housing (toward the base) until it is securely positioned over the circuit board and base.
5. While holding the circuit board cover in place, turn the panel back over until the LCD lies facedown on a soft cloth and the under-side of the base is exposed.
6. Insert and secure the four Housing Screws (using a grounded Phillips-head screwdriver) in their respective locations, as shown in FIG. 18 on page 21.
7. Replace any adhesive plastic "feet" that might have been removed during the removal process of the outer housing. *These "feet" must be placed back onto their original locations so they can fit into their provided openings on the Battery Base.*
8. Grasp both the LCD and housing and then rotate the entire unit back onto a flat surface.
9. Insert all connectors and apply power.

Installation and Upgrade of the Internal NXD Components

Upgrading the cards within the WallMount panel involves removing the rear plastic outer housing (back box), removing the existing card, replacing it with the 802.11g upgrade, and then placing the back box back onto the NXD panel, as described in the following sections.

These panels do not come factory installed with the NXA-WC802.11GCF wireless interface card. This card must be ordered separately from AMX as part of the 802.11g upgrade kit (**FG2255-07**).

Step 1: Remove the existing NXD Outer Housing

1. Carefully detach all connectors from the side of the touch panel and remove the Faceplate from the front of the panel.
2. Place the LCD facedown on a soft cloth to expose the under-side of the unit (FIG. 24). This step helps prevent scratching of the LCD.

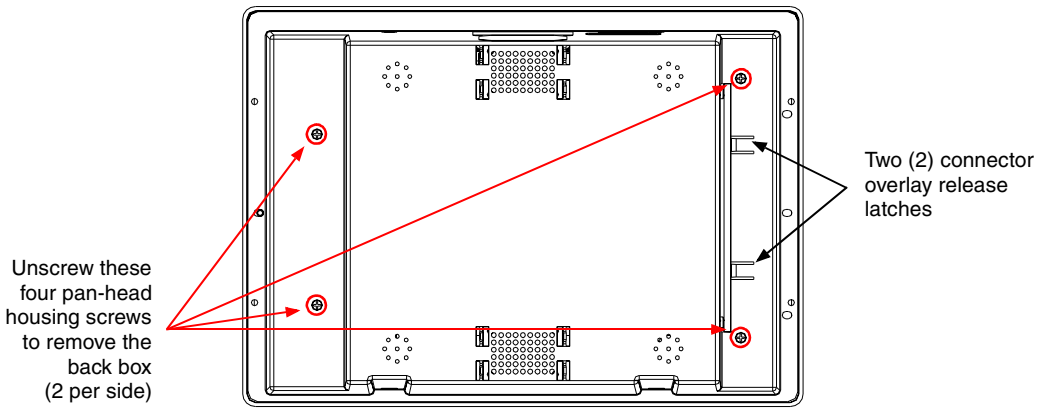


FIG. 24 Location of the attachment screws and connector overlay release latches on an NXD back box

3. Firmly press down on both connector overlay release latches (located in front of the connectors). *Pressing down releases the connector overlay from atop the connectors.*

NOTE

The overlay connector must first be released before the rear back box can be removed from the NXD-CV7 panel.

4. Gently slide the connector overlay away from the back box housing.
5. Unscrew the outer housing (back box) by using a grounded Phillips-head screwdriver to remove the two sets of pan-head Housing Screws, located on both sides of the housing (FIG. 24).

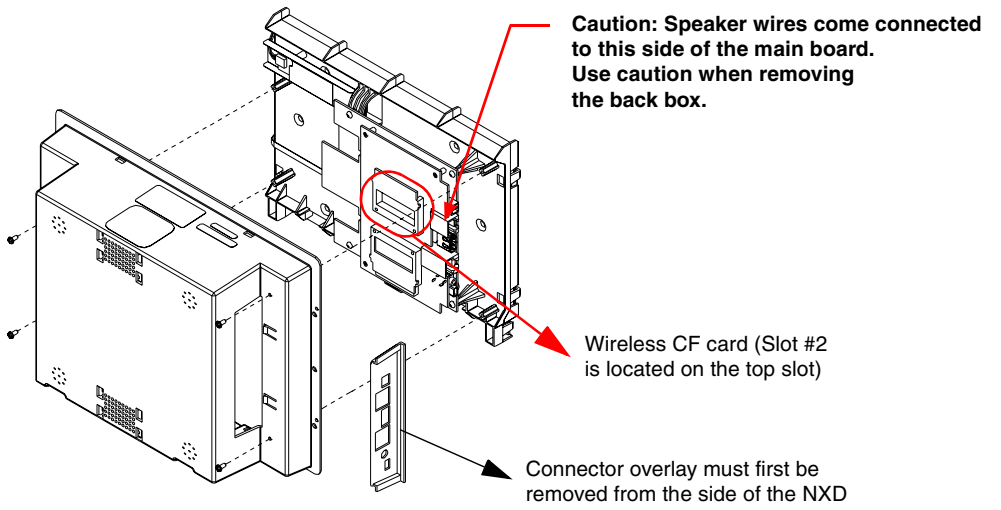

Caution: Speaker wires come connected to this side of the main board. Use caution when removing the back box.
Wireless CF card (Slot #2 is located on the top slot)
Connector overlay must first be removed from the side of the NXD

FIG. 25 Location of the wireless CF card connector on main board

CAUTION

The circuit board comes pre-wired to internal speakers located on the inside surface of the rear back box. If the back box is removed incorrectly, these speaker wires can become disconnected and damaged.

6. Carefully lift-off the back box housing and angle it over to the side of the unit where the wires are connected to the circuit board.
7. Gently lay the back box to one side of the unit. This exposes the internal circuit board (FIG. 25). Take care not to place undue strain on the speaker cables.

Step 2: Install the new Compact Flash Memory card (NXD)

1. Complete the procedures outline within *Step 2: Install the Compact Flash Memory card upgrade* section on page 22 and then continue with the following Step 3.

Step 3: Install the new 802.11g Wireless Compact Flash card (NXD)

Complete the procedures outline within *Step 3: Install the new 802.11g CF Card and Antenna* section on page 24 and then continue with the following Step 4.

Step 4: Close and Resecure the NXD Panel Enclosure

1. Gently place the outer housing back onto the panel and align the four pan-head Housing Screws holes along the edges of the outer housing.
2. Insert and secure the four pan-head Housing Screws back into their pre-drilled holes by using a grounded Phillips-head screwdriver.
3. Slip the connector overlay back into the connector opening by inserting the top of the overlay into the connector opening in an upwards direction.
4. Align the connectors to their respective locations and secure the overlay by pushing it towards the connectors until the overlay securely snaps back into the overlay release latches.
5. Re-install the faceplate back onto the panel. Refer to the *Installing the No-Button Trim Ring* section on page 35 for more detailed faceplate installation information.

NXT-BP Power Pack (FG2255-10)

The NXT-BP Power Pack (FIG. 26) is a rechargeable Lithium-Ion "smart" battery used to provide power to the NXT Modero panel through the NXA-BASE/1 Battery Base. This battery incorporates an on-board battery life indicator. The NXT-BP battery can be charged through either the base (when connected to the CV10 panel) or through an optional NXT-CHG Modero Power Station.

Although this product is included within the NXA-BASE/1 Kit (Fg2255-05K), extra NXT-BP Power Packs (**FG2255-10**) can be purchased separately as an optional accessory.

FIG. 26 NXT-BP Power Pack

NXT-BP Specifications	
Dimensions (HWD):	• 0.69" x 3.50" x 5.81" (1.75 cm x 8.89 cm x 14.76 cm)
Power (Voltage):	• 11.1 Volts (nominal)
Weight:	• Single NXT-BP Power Pack: 1.0 lbs (0.45 kg)
Features:	• Battery Usage: 4 to 8 hours (time is usage dependant) • Charge Capacity: 6300mAh
Operating / Storage Environment:	• Operating Temperature: 0° C (32° F) to 40° C (104° F) • Operating Humidity: 20% - 85% RH • Storage/Discharge Temperature: -20° C (-4° F) to 60° C (140° F) • Storage Humidity: 5% - 85% RH

NXA-BASE/1 Battery Base Kit (FG2255-05K)

The NXA-BASE/1 Kit contains a single NXT-BP battery and one battery base. The NXA-BASE/1 (FIG. 27) is a Modero accessory that allows an NXT-CV10 touch panel to function off the charge from a single internally connected NXT-BP battery. The base provides both power and battery information to the panel via the panel interface connector. The NXT-BP battery can be charged through either the base (only when connected to the NXT-CV10 touch panel) or through an optional NXT-CHG Modero Power Station Kit (**FG2255-50K**). When used with the optional battery base, the CV10 panels will charge the battery during full operation.

FIG. 27 NXA-BASE/1 Kit (consists of one BASE/1 and a single NXT-BP)

NXA-BASE/1 Specifications	
Dimensions (HWD):	• 0.93" x 5.96" x 6.89" (2.36 cm x 15.14 cm x 17.51 cm)
Power Requirements:	• 1.4 A @ 12 VDC (max power draw while charging a single battery)
Weight:	• Base unit: 0.75 lbs (0.34 kg) • Base and 1 battery: 1.75 lbs (0.79 kg)
Features:	• Charge time for single depleted battery: ~ 5 - 8 hours • Must be connected to a Modero unit utilizing a 12 VDC-compliant power supply
Operating / Storage Environment:	• Operating Temperature: 0° C (32° F) to 40° C (104° F) • Operating Humidity: 20% - 85% RH • Storage Temperature: -20° C (-4° F) to 60° C (140° F) • Storage Humidity: 5% - 85% RH
Included Accessories:	• NXA-BASE/1 (**FG2250-05k**): 1 battery base and 1 NXT-BP battery
Other AMX Equipment:	• NXT-CHG Kit (**FG2250-50K**): 1 charger and 2 NXT-BP batteries • NXT-BP battery pack (**FG2255-10**) (additional)

NOTE

Before beginning the installation of the battery base to the Modero panel, verify the Modero panel has the latest firmware. Only the latest build incorporates the necessary updates for using the Modero with the NXA-BASE/1. From the Battery Base page, verify that the battery base is loaded with the latest NXA-BASE/1 firmware (v2.xx or higher).

Checking the NXT-BP charge

1. Press the Battery Life Indicator button (FIG. 28) once to illuminate the Battery Life LEDs and display the percent charge remaining on the battery (this indication lasts a few seconds).

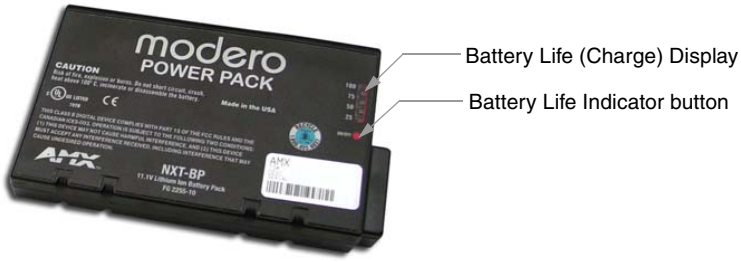


FIG. 28 NXT-BP Battery Pack (showing the battery life indicator and button)

2. Charge the NXT-BP battery by either inserting it into the battery base or from within the optional NXT-CHG charger (which can sequentially charge up to two batteries).

NOTE

It is recommended to fully charge this battery before using it to power an NXT-CV10 panel. If the 25% LED indicator is blinking, recharge your battery immediately. This blinking indicates there is less than 5% of a charge remaining on the battery.

Installing an NXT-BP into the NXA-BASE/1

The base does not directly connect to a power supply. Instead, it receives the power necessary to charge the battery from the Modero panel (through the Panel Interface connector).

1. Install the NXT-BP battery into the base's battery compartment with the label-side facing up.
2. Align the battery connector with its corresponding battery connector port (located in the battery compartment shown in FIG. 29).

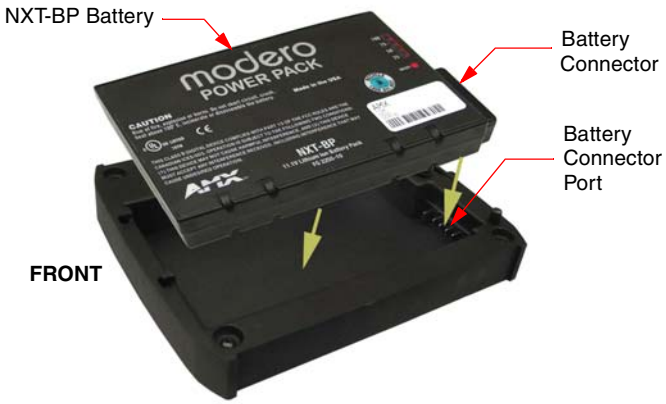


FIG. 29 Battery installation

3. Carefully insert the NXT-BP into the base until the battery securely fits onto the Battery Connector Port.

Installing the NXA-BASE/1 below an NXT-CV10 Panel

1. Power Off the panel before attempting to attach the NXA-BASE/1.
2. Place the battery base (with battery) onto a flat/level surface.
3. Turn the battery locking slider (FIG. 30) to one side until the locking mechanism is horizontal to the base (going left to right) and the rear battery latch is pointing directly outward (away from the LCD).
4. Carefully angle the NXT-CV10 panel over the front alignment pegs (FIG. 31). The pegs assist in both aligning and securing the panel to the base (the locking mechanism secures the base to panel when done).
5. Insert the alignment pegs into their corresponding holes below the front of the panel.
6. Verify the alignment of the Panel Interface connectors between the panel (female connector) and base (male connector) (FIG. 31).
7. Align the rear pegs and gently push the rear of the panel downwards until it is mounted atop the battery base.

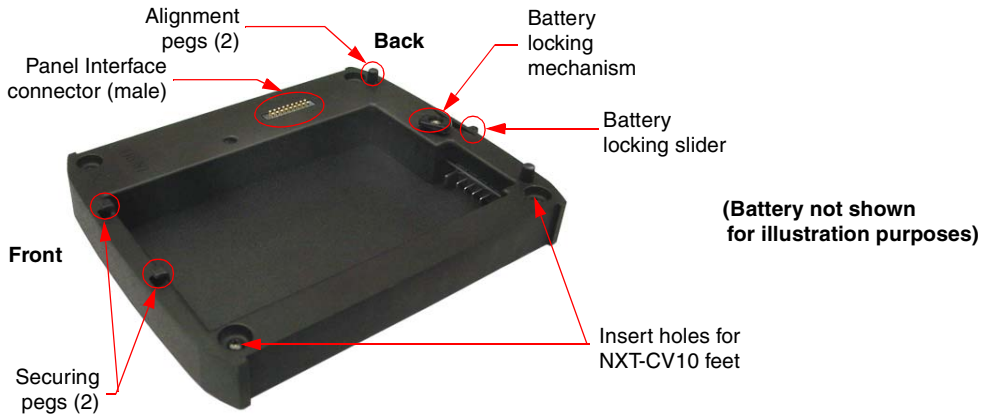


FIG. 30 NXA-BASE/1 showing Panel Interface and connector locations

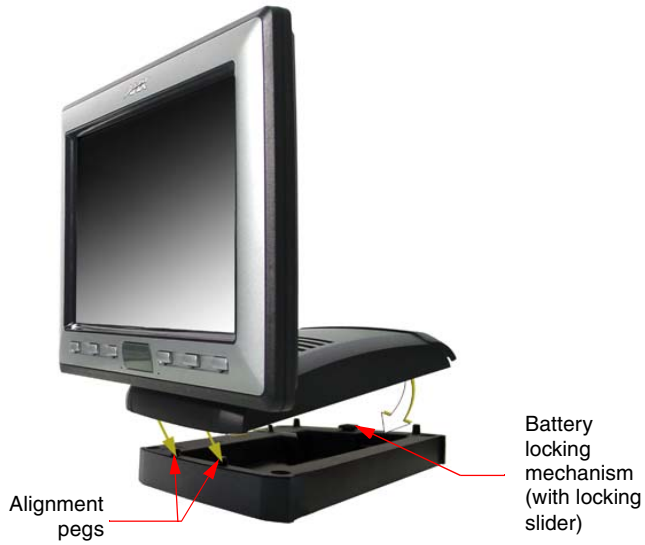


FIG. 31 NXA-BASE/1 shown aligning with NXT-CV10 panel

CAUTION

The battery base CANNOT be hot-swapped. An NXT can not be receiving power (through a connected power supply) and then be connected to a battery base. Always POWER OFF the panel before installing the NXA-BASE/1.

8. Slide the rear battery locking slider in the opposite direction. This turns the latching mechanism and secures the panel to the base.
9. Upon successful connection, the AMX logo appears on the panel to indicate that the panel is properly connected and receiving power.

Charging the NXT-BP using the NXA-BASE/1

1. Insert the single battery into the battery compartment shown in FIG. 30 on page 31.
2. Follow the procedures from the previous sub-section to attach the NXT-CV10 to the NXA-BASE/1.
3. Insert a 2-pin connector from a power supply to the rear PWR connector on the NXT-CV10 Modero panel. Refer to the *Battery Base Page* section on page 98 to view the charging progress of the connected NXT-BP.

NXT-CHG Battery Charger Kit (FG2255-50K)

The NXT-CHG Kit includes one charger and two NXT-BP batteries. The optional NXT-CHG Modero Power Station (FIG. 32) is a two-slot, stand-alone battery charger that can be used to recharge up to two NXT-BP batteries. The batteries are charged in the order they are inserted into the charger. The NXT-CHG Slot 1 has the feature of being able to completely discharge and recharge (*recalibrate*) a battery.

FIG. 32 NXT-CHG Kit (consists of one NXT-CHG charger and two NXT-BP batteries)

NXT-BP and NXT-CHG Specifications	
Dimensions (HWD):	• 1.13" x 8.63" x 11.81" (2.86 cm x 21.91 cm x 30.00 cm)
Power Requirements:	• NXT-BP Battery Voltage - 11.1 Volts • NXT-CHG: 90 - 264 VAC, 47-63 Hz, Single Phase (using the included 24 VDC power supply)
Weight:	• 0.57 lbs (0.26 kg)
Features:	• Charge time for two depleted batteries: ~ 5 hours • Charge Rate: 2.5 A @ 12 VDC • 2-Bays: Sequential charging • LED: One LED indicator in front of each bay which conveys the status of that bay. Refer to the *Reading the NXT-CHG LED Indicator* section for more information. • Recalibration pushbutton (located between the bays): Initiates recalibration sequence in the **left bay only**. • Recalibration Time: less than 9 hours
Other AMX Equipment:	• NXT-CHG Kit (**FG2250-50K**): - 1 charger and 2 NXT-BP batteries • NXT-BP battery pack (**FG2255-10**) (additional)

The batteries are charged in the order they are inserted into the NXT-CHG. SLOT 1 of the NXT-CHG has the ability to completely discharge and recharge (*recalibrate*) a battery.

Powering the NXT-CHG

NOTE

Recalibration improves the reporting accuracy of the battery charge back to the Modero panel.

The NXT-CHG Smart Battery Charger uses an included power supply to charge inserted batteries.

1. Connect the rear of the NXT-CHG to the power adapter.
2. Connect the power adapter to the provided power cord (*with plug*).
3. Provide power to the unit by connecting the power cord (*with plug*) into a power outlet that meets the requirements outlined in the *Specifications* section for the NXT-CHG.

Reading the NXT-CHG LED Indicator

FIG. 33 shows the components on the NXT-CHG Smart Battery Charger.

FIG. 33 Component locations on the NXT-CHG

There is one LED indicator on the front of each battery slot that indicates the status of that slot. The blink patterns for these LEDs are described in the following table:

- **Off**: No battery detected.
- **Green Flashing**: Fast charging.
- **Green Solid**: Fully charged.
- **Yellow Flashing**: Recalibration in process.
- **Yellow/Green**: Recalibration complete.
- **Yellow Solid**: Standby (waiting for other battery to charge).
- **Red Flash**: Error (problem with either the battery connection to the internal slot, or with the battery itself).

Charging the NXT-BP batteries using the NXT-CHG

1. Review the *Checking the NXT-BP charge* section on page 29 to confirm the percentage of charge remaining on the batteries.
2. Provide power to the charger (as outlined in the *Powering the NXT-CHG* section on page 33).
3. Align the battery connector with the corresponding charge slot.
4. Firmly insert the battery into the desired slot until the battery is both securely located within the slot and there is activity from the corresponding Slot LED. Refer to the *Reading the NXT-CHG LED Indicator* section on page 33 section for LED information.

Recalibrating the batteries

The recalibration process increases the accuracy of the battery charge level. Recalibration of the batteries is only done upon a user request from the Modero on-screen Battery Base page.

Recalibration can only be done within Slot 1 on the NXT-CHG.

1. Place the selected battery securely into Slot 1 (left slot) until there is activity on the Slot 1 LED.
2. Push the **Recalibration** pushbutton (located between the two slots) to initiate recalibration in the left bay only.

Installation

NXT panels are mounted onto flat (horizontal) surfaces in either a stand-alone or combo (NXT atop an NXA-BASE/1 battery base) configuration. NXD panels are installed into either a pre-wall surface (using a CB-TP10 conduit/wallbox) or a solid surface (using either solid surface or drywall screws).

NOTE

It is recommended that if you are planning on upgrading your panel components (flash and wireless), you do so before beginning any panel installations.

Unpacking the Panel

1. Inspect and confirm the contents of the shipment box to verify you have all specified parts. Refer to the *Specifications for 10" Widescreen Video Touch Panels* section on page 3 for more information about included accessories and other AMX equipment.
2. Carefully remove the panel from the shipping box.
3. Carefully peel the protective plastic cover from the LCD.

NOTE

If the protective plastic LCD cover is not removed, the panel may not respond properly to touch points on the LCD or allow proper screen calibration.

Installing the Internal Components

Installation of the internal components such as the upgraded Compact Flash and the NXA-WC80211B/CF Wireless card are described in detail within the following sections:

- *NXA-WC80211GCF 802.11g Wireless Card (FG2255-07)* section on page 17.
- *NXA-CFSP Compact Flash (FG2116-3x)* section on page 20.

Installing the No-Button Trim Ring

The NXD-CV10 panel is shipped from AMX with a default Button Trim Ring already installed. The unit is also shipped with an included Trim Ring containing no button openings (a No-Button Trim Ring) that allows you, if desired, to change the default configuration of the NXD panel Faceplate to that with no-button openings. In order to install this included No-Button Trim Ring, you must first remove the factory-installed default Button Trim Ring, the six small buttons, and associated two clear light pipes.

1. The Faceplate is secured to the panel with plastic latches. To remove the Faceplate, simply pull it away from the panel by gently tugging it outwards until the entire Faceplate comes away from the panel.
2. Turn the Faceplate over to expose the inside surface and view the Trim Ring latches (FIG. 34).
3. In a single motion, press down and then outwards on the three Trim Ring latches located along the top of the internal surface of the Faceplate to begin removing the Button Trim Ring. *Removing the Internal Faceplate from the panel exposes the pushbuttons and light pipes along the inside of the Internal Faceplate.*
4. Gently tug along the edges of the Button Trim Ring and work your way around the edges to remove it from the Faceplate (FIG. 34).
5. From along the internal surface of the Faceplate, remove the six buttons by gently bending each Button latch up and pulling the button outwards.

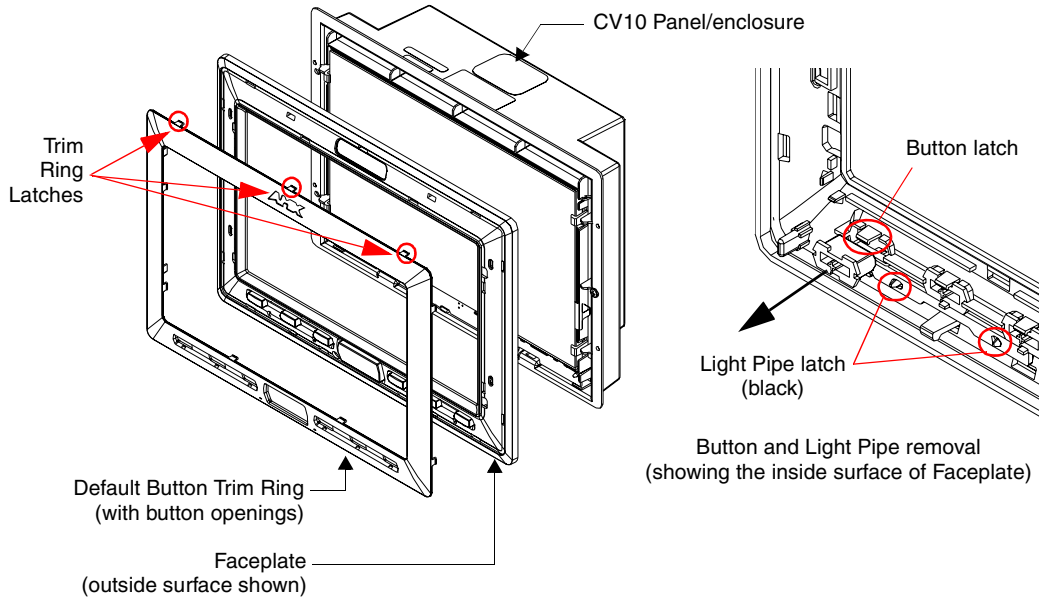


FIG. 34 Removing the default Button Trim Ring

6. Remove the pair of clear light pipe strips by bending the two black light pipe latches inwards and pulling out the strip.
7. Grasp the No-Button Trim Ring on both sides and fit it into the groove along the outside surface of the Faceplate (made available by the removal of the previous Trim Ring).
8. Gently insert the Trim Ring latches into their corresponding openings on the outer surface of the internal Faceplate (FIG. 35).

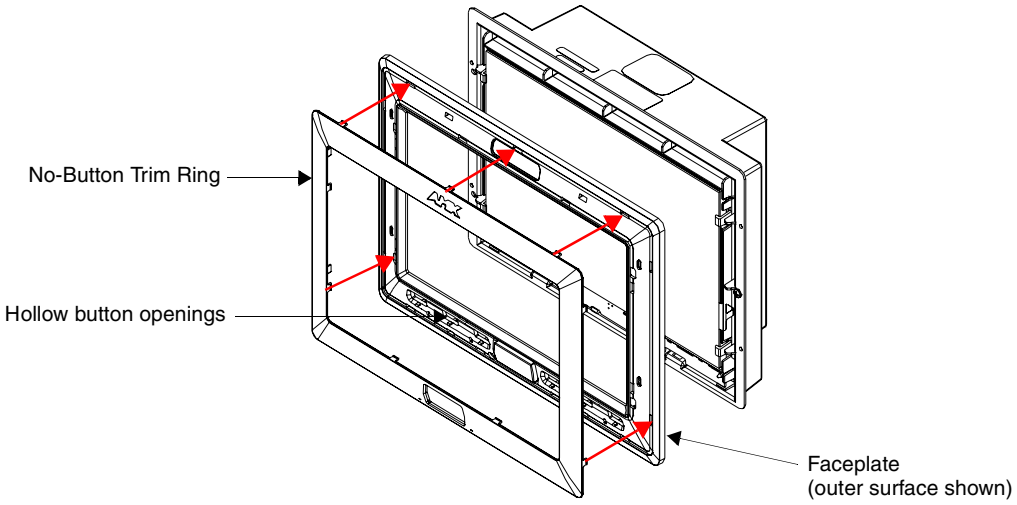


FIG. 35 Inserting the new No-Button Trim Ring

9. Firmly press down around the No-Button Trim Ring until all of the latches are securely inserted into their openings on the Faceplate, and the No-Button Trim Ring is securely fastened. Verify the No-Button Trim Ring is firmly inserted onto the Faceplate and that there are no gaps between this Trim Ring and the outer surface of the Faceplate.

10. Place the Faceplate back onto the main NXD-CV10 unit. Make sure to align the Microphone, Light, and PIR Motion sensor locations on the main unit to their respective openings on the Faceplate assembly.

Installing the Button Trim Ring

The outer No-Button Trim Ring is secured to the Faceplate with plastic latches. In order to re-install the Button Trim Ring back onto an NXD panel which has had the default Button Trim Ring features removed; you must first remove the No-Button Trim Ring:

1. To remove the Faceplate, simply pull it away from the panel by gently tugging it outwards until the entire Faceplate comes away from the panel.
2. Turn the Faceplate over to expose the inside surface and view the Trim Ring latches.
3. In a single motion, press down and then outwards on the three Trim Ring latches located along the top of the internal surface of the Faceplate to begin removing the Trim Ring. *Removing the Internal Faceplate from the panel exposes the pushbuttons openings left from an earlier removal of the pushbuttons and light pipes.*
4. Gently tug along the edges of the No-Button Trim Ring and work your way around the edges to remove it from the Faceplate (FIG. 36).

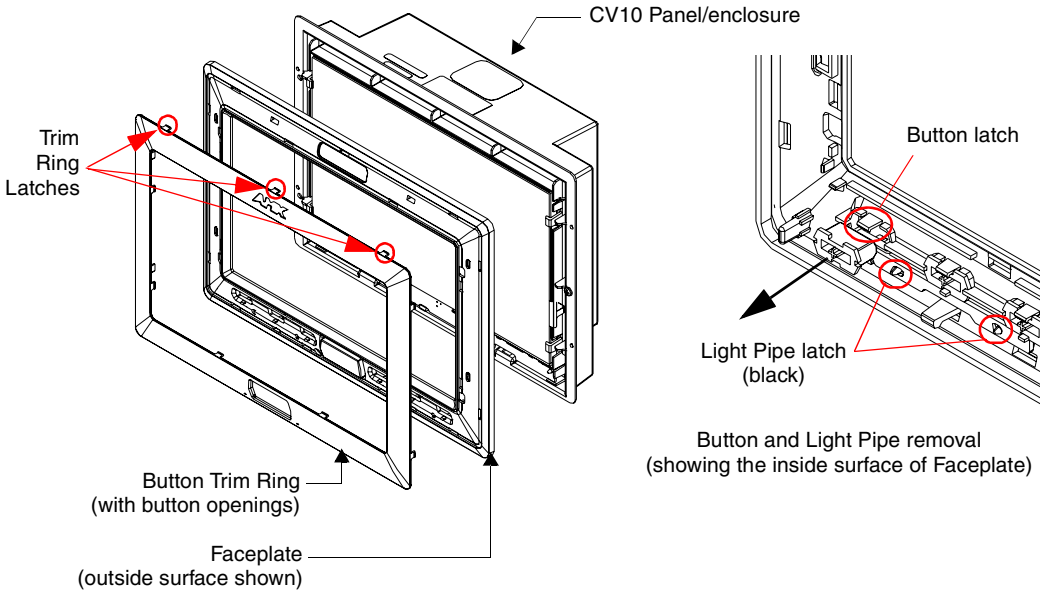

CV10 Panel/enclosure
Trim Ring Latches
Button latch
Light Pipe latch (black)
Button and Light Pipe removal (showing the inside surface of Faceplate)
Button Trim Ring (with button openings)
Faceplate (outside surface shown)

FIG. 36 Removing the No-Button Trim Ring

5. From along the internal surface of the Faceplate, install the six buttons by firmly inserting them into the button openings until the Button latch secures the button in place (FIG. 36).
6. Install the pair of clear light pipe strips by pushing light pipes over the two black light pipe latches.
7. Grasp the Button Trim Ring on both sides and fit it into the groove along the outside surface of the Faceplate (made available by the removal of the previous Trim Ring).
8. Gently insert the Button Trim Ring latches into their corresponding openings on the outer surface of the internal Faceplate (FIG. 37).
9. Firmly press down around the Button Trim Ring until all of the latches are securely inserted into their openings on the Faceplate, and the Button Trim Ring is securely fastened. Verify the Button Trim Ring is firmly inserted onto the Faceplate and that there are no gaps between this Trim Ring and the outer surface of the Faceplate.

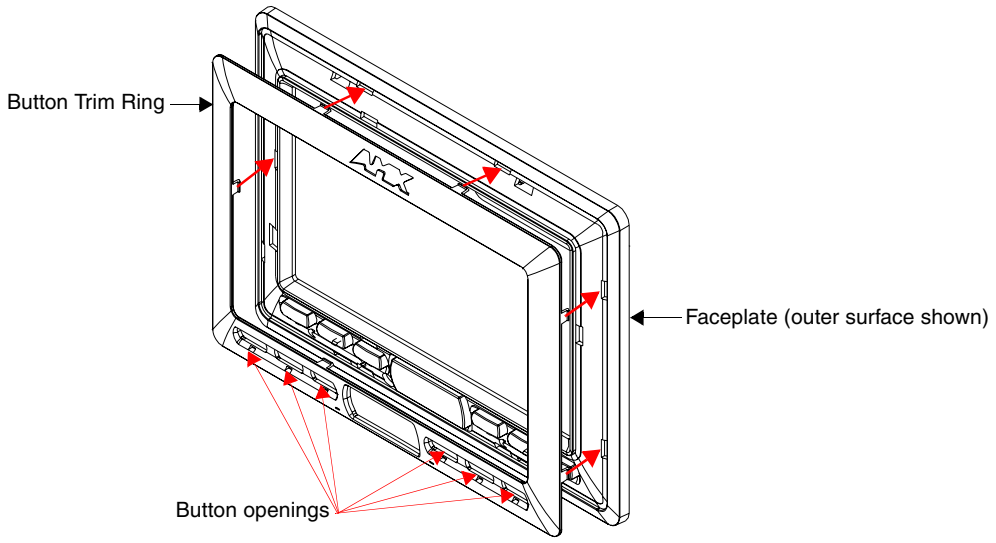


FIG. 37 Inserting the Button Trim RIng

10. Place the Faceplate back onto the main NXD-CV10 unit. Make sure to align the Microphone, Light, and PIR Motion sensor locations on the main unit to their respective openings on the Faceplate assembly.

Pre-Wall Installation of the Conduit Box

Wall Mount panels (NXDs) are contained within an outer housing (back box). This back box is **not** removed when installing the NXD into a Conduit Box (CB-TP10). The back box is ***only*** removed to gain access for the replacement of the internal components.

WARNING

INSTALLER: LEAVE A GAP BETWEEN THE STUD AND CONDUIT BOX MOUNTING TABS TO ACCOMMODATE THE DRYWALL or SHEETROCK.
This gap allows the installation of the drywall or sheetrock after the CB-TP10 Conduit Box has been installed.

The CB-TP10 is an optional metallic box that is secured onto a stud/beam in a **pre-wall** setting (*where no walls are present*). Installation procedures and configurations can vary depending on the installation environment. This section describes the installation procedures for the most common installation scenario. The most important thing to remember when mounting this conduit box is that the NXD-CV10 Mounting Tabs must lie flush against the outside of the sheetrock (FIG. 38).

- Refer to **SP-2259-02** for detailed installation dimensions.
- It is recommended that you cut out the surface slightly smaller than what is outlined in the installation drawings so that you can make any necessary cutout adjustments.
- The wiring knockouts on the left side will be used for the NXD-CV10 Wall Mount panel connectors, so always secure the conduit box to the stud using the Stud Mounting Holes on the right side of the box.

1. Rest the right Stud Mounting tabs onto the stud (keeping the knockouts on the left). **Be sure to leave enough of a gap between the stud and NXD Mounting tabs to accommodate the installation of the drywall or sheetrock after the conduit box has been mounted. Ultimately, the Mounting Tabs should lie flush against the outside of the sheetrock.**
2. Fasten the CB-TP10 conduit box to the stud through the holes on the right Stud Mounting tabs (FIG. 38), using either nails or screws.

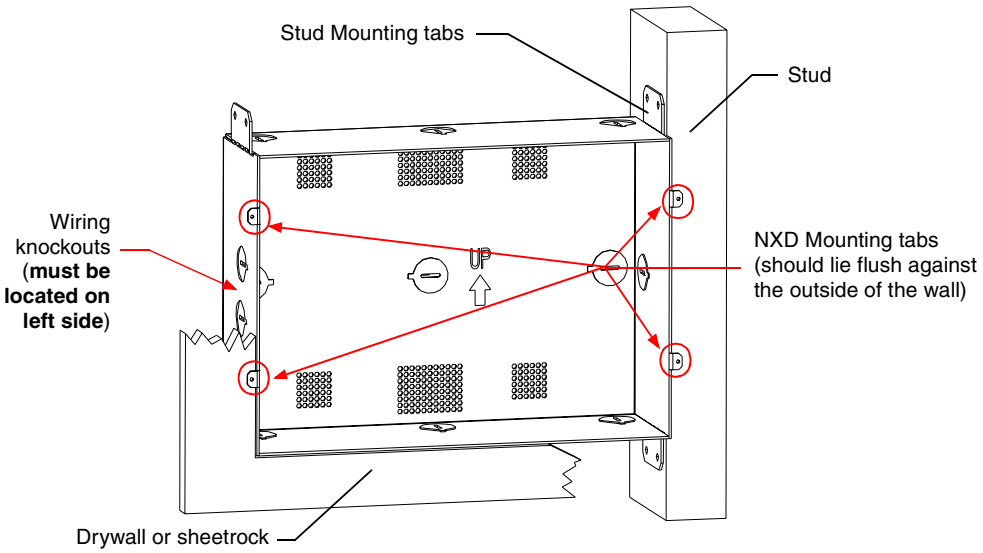

Stud Mounting tabs
Stud
Wiring knockouts (must be located on left side)
NXD Mounting tabs (should lie flush against the outside of the wall)
UP
Drywall or sheetrock

FIG. 38 CB-TP10 conduit box components

3. Remove the wiring knockouts from the left side of the conduit box (CB-TP10) (FIG. 38) to accommodate the cables being threaded through to the NXD touch panel.

NOTE

Remember that when mounting this conduit box, the NXD mounting tabs must lie flush against the outside of the sheetrock.

4. Thread the incoming power, RJ-45 audio/video, Ethernet, and USB wiring through the knockouts (***use of the left wiring knockouts are recommended with this installation***). Leave enough slack in the wiring to accommodate any re-positioning of the panel.
5. Install the drywall/sheetrock before inserting the main NXD unit into the CB-TP10.

Installation of an NXD Touch Panel

The NXD-CV10 can be installed either directly into the (optional) CB-TP10 or other solid surface environment using the two different mounting options: drywall clips or solid surface screws. The following sections describe mounting the touch panel directly into a pre-wall conduit box, a solid surface or drywall, and optional NXA-RK10 Rack Mount Kit for installation.

Installing the NXD panel within a Conduit Box

The conduit box must be mounted prior to continuing this section. Refer to the procedures in the *Pre-Wall Installation of the Conduit Box* section on page 38 for detailed pre-wall installation instructions. *Verify that all necessary cables have been threaded through the knockouts on the left of the conduit box and the connections have been tested prior to installation of the NXD-CV10.*

1. Remove the Faceplate/bezel (**A** in FIG. 39) from the main NXD unit (**B** in FIG. 39) by gripping the faceplate and pulling with gentle outward force.
2. Verify the incoming power, RJ-45 audio/video, Ethernet, and USB cables have been properly threaded through the wiring knockouts on the left of the conduit box. *Leave enough slack in the wiring to accommodate any re-positioning of the panel.*
3. Connect all data and power wiring connectors to their corresponding locations along the side of the (un-powered) NXD touch panel.

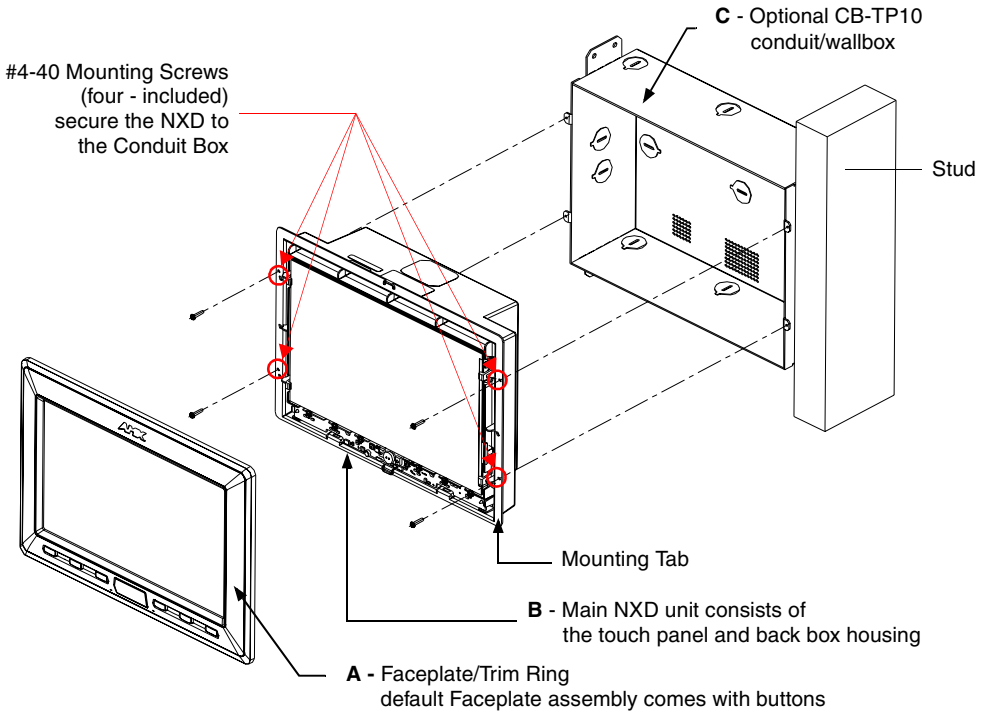


FIG. 39 NXD-CV10 panel installation into a CB-TP10 (pre-wall construction)

- Verify that the terminal end of the power cable is not connected to a power source before plugging in the 2-pin power connector.
- The USB connectors can be from either a USB extension cable, or a wireless USB RF transmitter.

4. Test the incoming wiring by connecting the panel connections to their terminal locations and applying power. Verify that the panel is receiving power and functioning properly to prevent repetition of the installation.
5. Disconnect the terminal end of the power cable from the connected power supply.

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the attached connectors before being inserted into the conduit box.

6. Carefully slide the main NXD-CV10 unit (**B** in FIG. 39) into the conduit box, so that all Mounting Tabs lie flush against the conduit box (**C** in FIG. 39).
7. Insert and secure four #4-40 Mounting Screws (included) into their corresponding holes located along the sides of the NXD.
8. Place the Faceplate/Trim Ring assembly (**A** in FIG. 39) back onto the main NXD unit (**B** in FIG. 39). *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front faceplate/bezel.*
9. Reconnect the terminal RJ-45, Ethernet, USB, and any optional audio/video wiring to their respective locations (*outside the conduit box*) on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
10. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Installing the NXD into drywall using Expansion Clips

Expansion clips are mounted through the three oval holes located along the rim of the NXD-CV10. As the screw is tightened, the clip bends toward the insertion hole and into the wall. This bending creates a "grip" on the wall by either pressing onto the wall or by securing the drywall between the housing and the drywall clip.

The most important thing to remember when mounting the NXD is that the outer frame (Mounting Tabs) must be installed flush against the mounting surface.

- Refer to **SP-2259-03** for detailed installation dimensions (reproduced in FIG. 40).
- It is recommended that you cutout the surface slightly smaller than what is outlined in the installation drawings so that you can make any necessary cutout adjustments.

1. Prepare the area by removing any screws or nails from the drywall before beginning the cutout process.g.
2. Cut out the drywall surface for the NXD Wall Mount unit using the dimensions shown in FIG. 40. Be sure to cut out the three notches along the sides to accommodate the three corresponding drywall expansion clips (included).

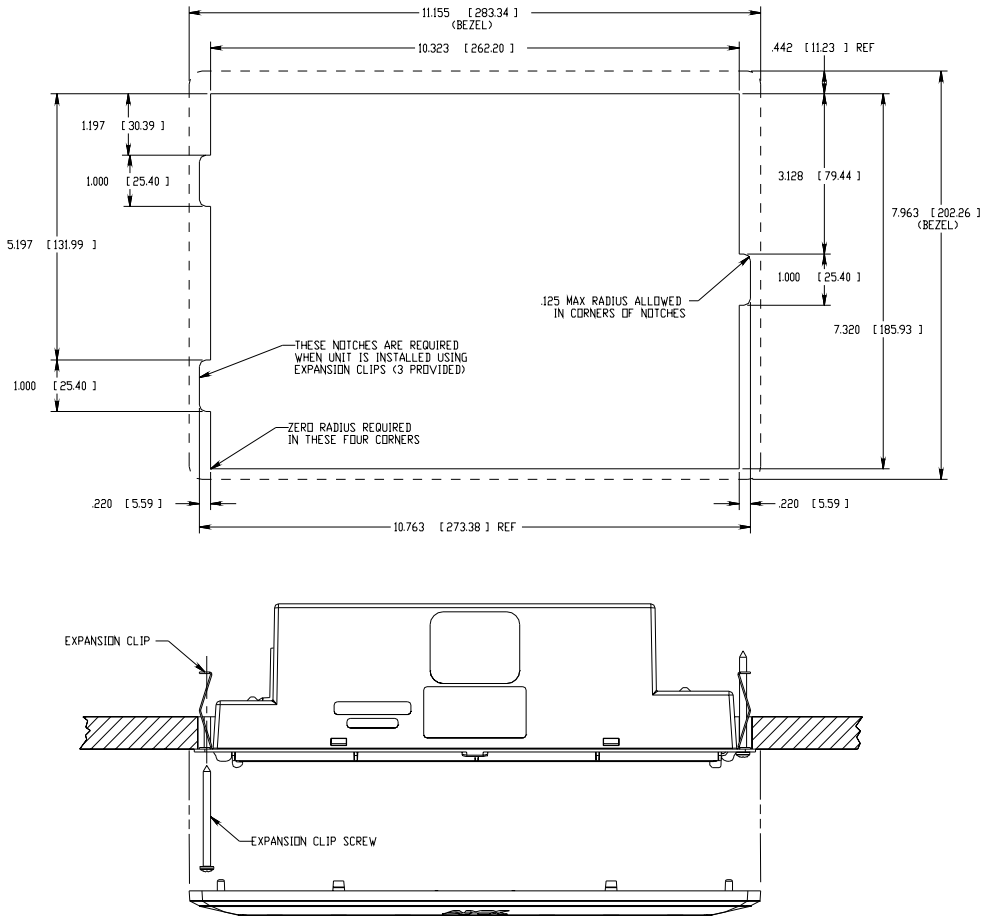


FIG. 40 NXD-CV10 Wall Mount panel dimensions using expansion clips

3. Remove the Faceplate/bezel (**A** in FIG. 41) from the main NXD unit (**B** in FIG. 41) by gripping the faceplate and pulling with gentle outward force.

4. Thread the incoming power, RJ-45, Ethernet, USB, and any optional audio/video wiring (from their terminal locations) through the surface opening. *Leave enough slack in the wiring to accommodate any re-positioning of the panel.*
5. Connect all data and power wiring connectors to their corresponding locations along the left side of the (un-powered) NXD touch panel.
   - Verify that the terminal end of the power cable is not connected to a power source before plugging in the 2-pin power connector.
   - The USB connectors can be from a either a USB extension cable, or a wireless USB RF transmitter.

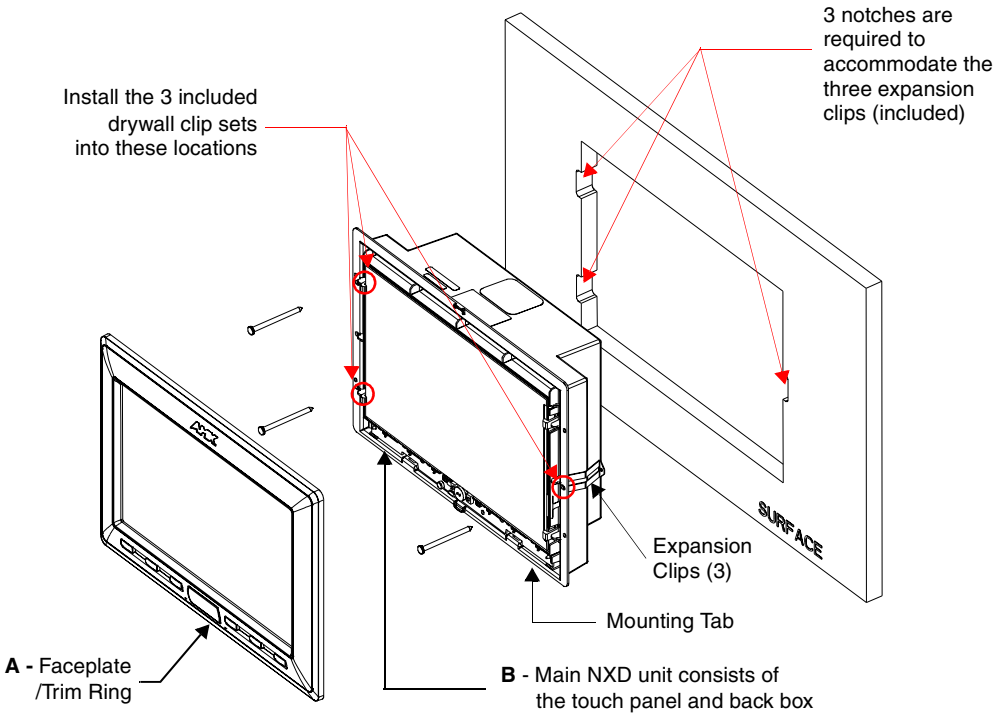

3 notches are required to accommodate the three expansion clips (included)
Install the 3 included drywall clip sets into these locations
SURFACE
Expansion Clips (3)
Mounting Tab
A - Faceplate /Trim Ring
B - Main NXD unit consists of the touch panel and back box

FIG. 41 Wall Mount panel (NXD) installation configuration for drywall surfaces

6. Test the incoming wiring by attaching the panel connections to their terminal locations and applying power. Verify the panel is receiving power and functioning properly to prevent repetition of the installation.
7. Disconnect the terminal end of the power cable from the connected power supply.

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the attached connectors before being inserted into the drywall.

8. Install the three sets of drywall screws and expansion clips into the three oval notch locations along both sides of the main unit (**B** in FIG. 41).
9. Carefully insert the main unit (with expansion clips) into the cutout until the Mounting Tabs on the NXD unit lie flush against the wall.

WARNING

The drywall clip set must be re-ordered from AMX if the drywall clip is bent accidentally during an installation or removed during a re-installation.

10. Tighten all three drywall clip sets (screws and clips) until the entire Mounting Tab is securely fastened and flush against the wall.
11. Place the Faceplate/Trim Ring assembly (**A** in FIG. 41) back onto the main NXD unit (**B** in FIG. 41). *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front faceplate/bezel.*
12. Reconnect the terminal RJ-45, Ethernet, USB, and any optional audio/video wiring to their respective locations on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
13. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Installing the NXD into a Flat Surface using #4 screws

Mounting screws (#4-40, included) are secured through two sets of circular holes located at the left and right sides of the NXD-CV10. **The most important thing to remember when mounting the NXD Wall Mount is that the outer frame (Mounting Tabs) must be installed flush against the mounting surface.**

- Refer to **SP-2259-03** for detailed installation dimensions (reproduced in FIG. 42).
- It is recommended that you cutout the surface slightly smaller than what is outlined in the installation drawings so that you can make any necessary cutout adjustments.

1. Prepare the area by removing any screws or nails from the surface before beginning the cutout process.
2. Cut out the surface for the NXD Wall Mount unit using the dimensions shown in FIG. 42.
3. Remove the Faceplate/bezel (**A** in FIG. 43) from the main NXD unit (**B** in FIG. 43) by gripping the faceplate and pulling with gentle outward force.
4. Thread the incoming power, RJ-45, Ethernet, USB, and any optional audio/video wiring (from their terminal sources) through the surface opening. *Leave enough slack in the wiring to accommodate any re-positioning of the panel.*
5. Connect all data and power wiring connectors to their corresponding locations along the left side of the (un-powered) NXD touch panel.
   - Verify that the terminal end of the power cable is not connected to a power source before plugging in the 2-pin power connector.
   - The USB connectors can be from a either a USB extension cable, or a wireless USB RF transmitter.
6. Test the incoming wiring by connecting the panel connections to their terminal locations and applying power. Verify that the panel is receiving power and functioning properly before finalizing the installation.
7. Disconnect the terminal end of the power cable from the power supply.

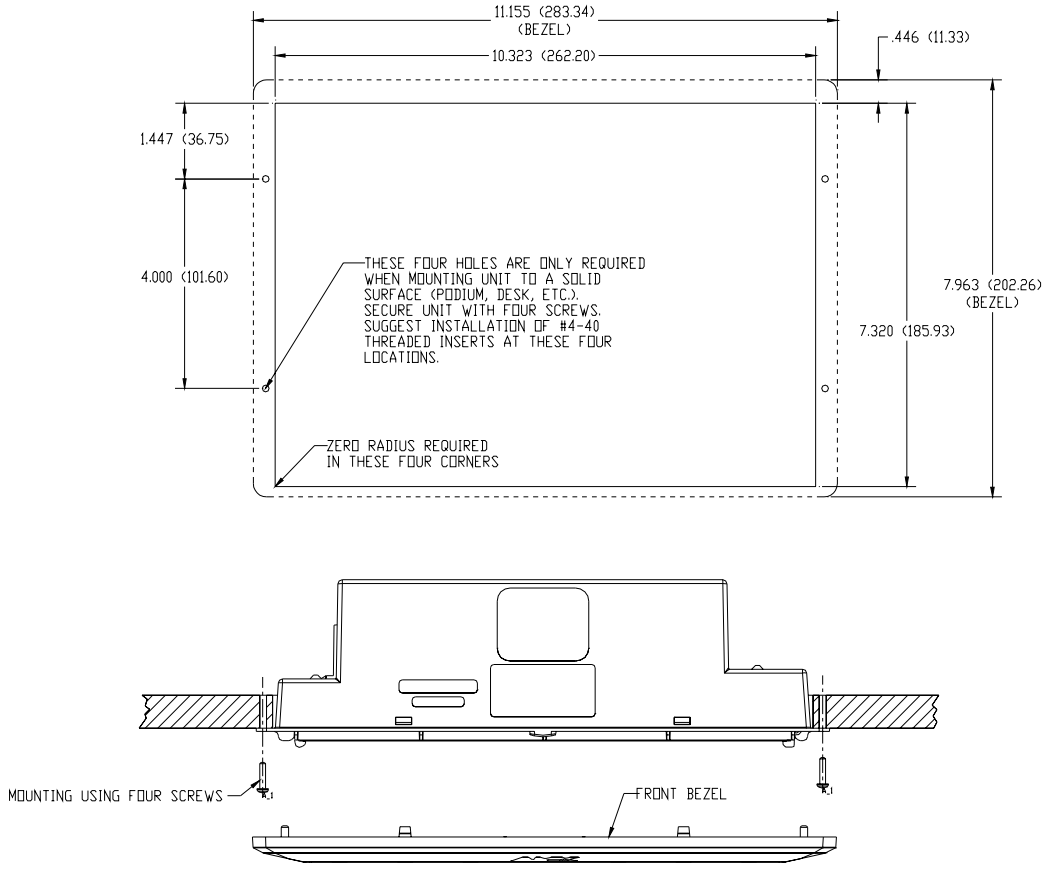

11.155 (283.34)
(BEZEL)
10.323 (262.20)
.446 (11.33)
1.447 (36.75)
4.000 (101.60)
THESE FOUR HOLES ARE ONLY REQUIRED WHEN MOUNTING UNIT TO A SOLID SURFACE (PODIUM, DESK, ETC.). SECURE UNIT WITH FOUR SCREWS. SUGGEST INSTALLATION OF #4-40 THREADED INSERTS AT THESE FOUR LOCATIONS.
7.963 (202.26)
(BEZEL)
7.320 (185.93)
ZERO RADIUS REQUIRED IN THESE FOUR CORNERS
MOUNTING USING FOUR SCREWS
FRONT BEZEL

FIG. 42 NXD-CV10 Wall Mount panel dimensions using #4-40 mounting screws

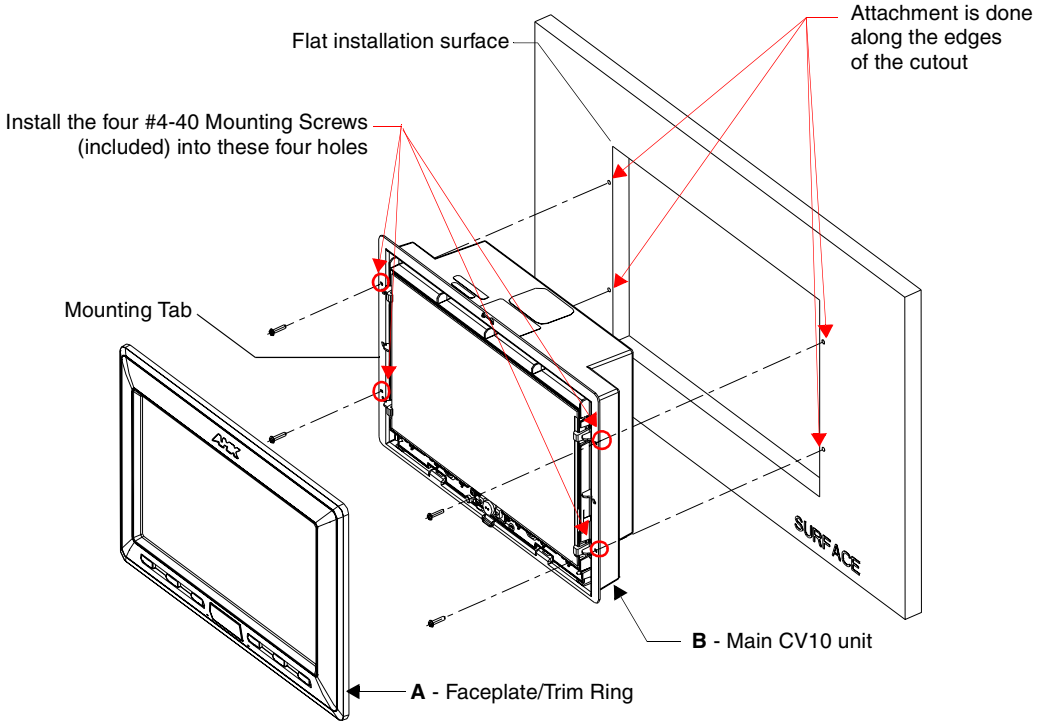

Flat installation surface
Attachment is done along the edges of the cutout
Install the four #4-40 Mounting Screws (included) into these four holes
Mounting Tab
SURFACE
B - Main CV10 unit
A - Faceplate/Trim Ring

FIG. 43 Wall Mount panel installation configuration for flat surfaces

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the necessary connectors before being inserted into the solid surface.

8. Carefully slide the main unit into the cutout until the Mounting Tabs of the CV10 unit lie flush against the wall.
9. Insert and secure four #4-40 Mounting Screws (included) into their corresponding holes located along the sides of the NXD-CV10 (using a grounded Phillips-head screwdriver) until the unit is secure and flush against the wall (FIG. 43).
10. Place the Faceplate/Trim Ring assembly (**A** in FIG. 43) back onto the main NXD unit (**B** in FIG. 43). *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front bezel/faceplate.*
11. Reconnect the terminal RJ-45, Ethernet, USB, and any optional audio/video wiring to their respective locations on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
12. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Installing an NXD-CV10 into an (optional) Rack Mount Kit (NXA-RK10)

The NXA-RK10 is a 8.72" (22.15 cm) wide high metal rack-mount (with black matte finish) measuring 5 RUs (rack units) high.

1. Remove the Faceplate/Trim Ring assembly from the main CV10 unit.
2. Thread the incoming power, RJ-45 audio/video, Ethernet, and USB wiring (from their terminal sources) through the surface opening, leaving enough slack in the wiring to accommodate any re-positioning of the panel.
3. Connect all data and power wiring connectors to their corresponding locations along the left side of the (un-powered) NXD touch panel.
   - Verify that the terminal end of the power cable is not connected to the a power supply before plugging in the 2-pin power connector.
   - The USB connectors can be from a either a USB extension cable, or a wireless USB RF transmitter.
4. Test the incoming wiring by connecting the panel connections to their terminal locations and applying power. Verify that the panel is receiving power and functioning properly to prevent repetition of the installation.
5. Disconnect the terminal end of the power cable from the connected power supply.

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the necessary connectors before being inserted into the equipment rack.

6. Carefully insert the CV10 panel into the NXA-RK10.
7. Secure the panel to the NXA-RK10 mount by first inserting and then tightening the four #4-40 screws (included).
8. Insert the NXA-RK10 (with connected NXD unit) into the equipment rack, making sure to align the screw holes along the sides on the NXA-RK10 with the holes in the equipment rack.
9. Use a grounded Phillips-head screwdriver to secure the NXA-RK10 to the equipment rack using #10-32 screws (included).

10. Place the Faceplate/Trim Ring assembly back onto the main NXD unit. *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front faceplate/bezel.*
11. Reconnect the terminal RJ-45 audio/video, Ethernet, and USB wiring to their respective terminal locations on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
12. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Wiring Guidelines for the CV10 Panels

CV10 panels use a 12 VDC-compliant power supply to provide power to the panel via the 2-pin 3.5 mm mini-Phoenix PWR connector. Use the power requirements information (page 3) to determine the power draw.

The incoming PWR and GND wires from the power supply must be connected to the corresponding locations within the PWR connector.

WARNING

These units should only have one source of incoming power. Using more than one source of power to the touch panel can result in damage to the internal components and a possible burn out.
*Apply power to the panels **only after** installation is complete.*

Preparing captive wires

You will need a wire stripper and flat-blade screwdriver to prepare and connect the captive wires.

WARNING

Never pre-tin wires for compression-type connections.

1. Strip 0.25 inch (6.35 mm) of insulation off all wires.
2. Insert each wire into the appropriate opening on the connector (according to the wiring diagrams and connector types described in this section).
3. Tighten the screws to secure the wire in the connector. Do not tighten the screws excessively; doing so may strip the threads and damage the connector.

Wiring a power connection

To use the 2-pin 3.5 mm mini-Phoenix connector for use with a 12 VDC-compliant power supply, the incoming PWR and GND wires from the external source must be connected to their corresponding locations on the connector (FIG. 44).

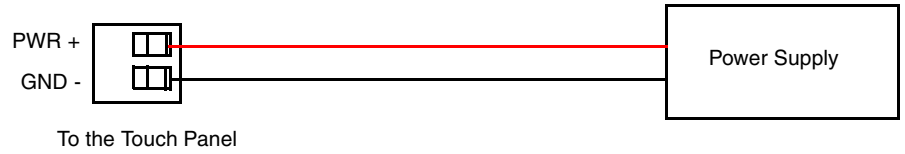


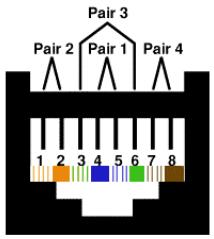
FIG. 44 NetLinx power connector wiring diagram

1. Insert the PWR and GND wires on the terminal end of the 2-pin 3.5 mm mini-Phoenix cable. ***Match the wiring locations of the +/- on both the power supply and the terminal connector.***
2. Tighten the clamp to secure the two wires. *Do not tighten the screws excessively; doing so may strip the threads and damage the connector.*
3. Verify the connection of the 2-pin 3.5 mm mini-Phoenix to the external 12 VDC-compliant power supply.

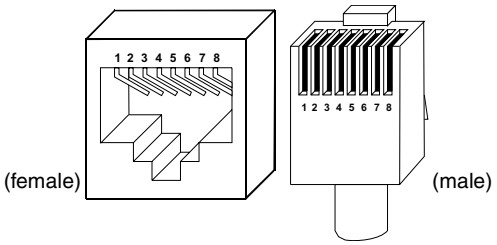
Audio/Video Port: Connections and Wiring

The following table shows the signal and pinout/pairing information used on the RJ-45 Audio and Video connections.

Audio/Video RJ-45 Pinout Information			
Pin	Wire Color	Function	Polarity
1	Orange/White	Right Audio In	+
2	Orange	Right Audio In	-
3	Green/White	Video In	-
4	Blue	Mic Out	-
5	White/Blue	Mic Out	+
6	Green	Video In	+
7	White/Brown	Left Audio In	+
8	Brown	Left Audio In	-



TIA 568B



RJ-45 connector - pin configurations

Ethernet/RJ-45 Port: Connections and Wiring

FIG. 45 describes the blink activity for the Ethernet 10/100 Base-T RJ-45 connector and cable. The Ethernet cable is connected to the rear of Table Top and side of the Wall Mount panels.

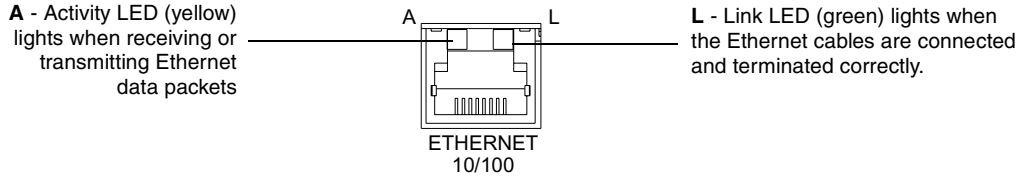

A - Activity LED (yellow) lights when receiving or transmitting Ethernet data packets
A
L
L - Link LED (green) lights when the Ethernet cables are connected and terminated correctly.
ETHERNET
10/100

FIG. 45 Ethernet connector (showing communication and connection LEDs)

The following table lists the pinouts, signals, and pairing associated with the Ethernet connector.

Ethernet RJ-45 Pinouts and Signals				
Pin	Signals	Connections	Pairing	Color
1	TX +	1 --------- 1	1 --------- 2	Orange-White
2	TX -	2 --------- 2		Orange
3	RX +	3 --------- 3	3 --------- 6	Green-White
4	no connection	4 --------- 4		Blue
5	no connection	5 --------- 5	4 --------- 5	Blue-White
6	RX -	6 --------- 6		Green
7	no connection	7 --------- 7	7 --------- 8	Brown-White
8	no connection	8 --------- 8		Brown

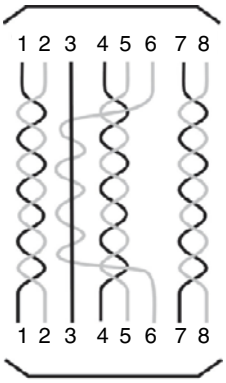


FIG. 46 diagrams the RJ-45 pinouts and signals for the Ethernet RJ-45 connector and cable.

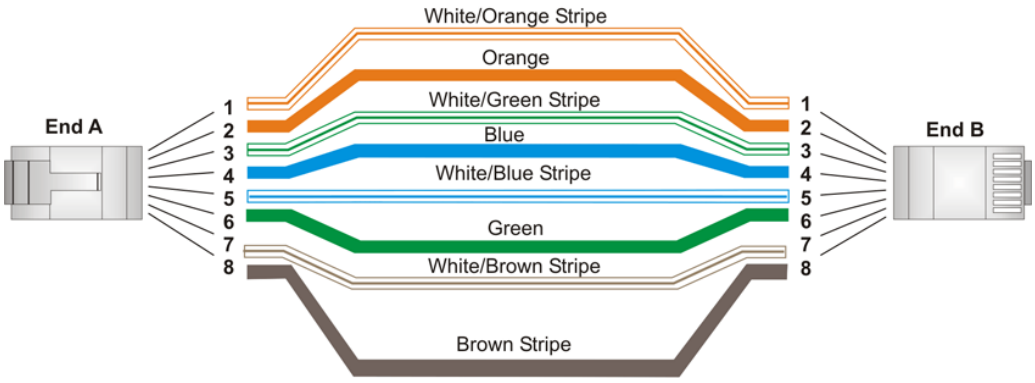


FIG. 46 RJ-45 wiring diagram

USB Port: Connecting and Using Input Devices

The CV10 panel can have up to two USB-capable input devices connected for use on its different firmware and TPD4 panel pages. These input devices can consist of a keyboard or mouse.

NOTE

USB-connected input devices are not detected and recognized by the panel until power is cycled to the unit.
A mini-USB connection is only detected after it is installed onto an active panel. Connection to a previously powered panel, allows the PC to detect the panel and assign an appropriate USB driver.

1. Insert the input device USB connectors into the appropriate USB connector on the panel.
2. Press the on-screen **Reboot** button from the Protected Setup page to save any changes and restart the panel.
3. After the panel splash-screen disappears:
   - If a USB mouse has been connected, a mouse cursor appears on the panel screen and its location corresponds to the mouse cursor position sent by the external USB mouse.
   - If a USB keyboard has been connected, only on-screen keyboards and keypads will reflect any external keystrokes sent from the external USB keyboard.

Panel Calibration

This section outlines the steps for calibrating the touch panel. *It is recommended that you calibrate the panel before its initial use and after completing a firmware download.*

Modero panels are factory setup with specific demo touch panel pages. The first splash screen that appears indicates the panel is receiving power, beginning to load firmware, and preparing to display the default touch panel pages. When the panel is ready, the AMX Splash Screen is replaced by the Initial Panel Page (FIG. 47).

FIG. 47 AMX splash screen and initial Panel Page

Calibrating the Modero Panel

1. Press and hold the grey Front Setup Access button (FIG. 48) for **6 seconds** to pass-over the Setup page and access the Calibration setup page (FIG. 49).

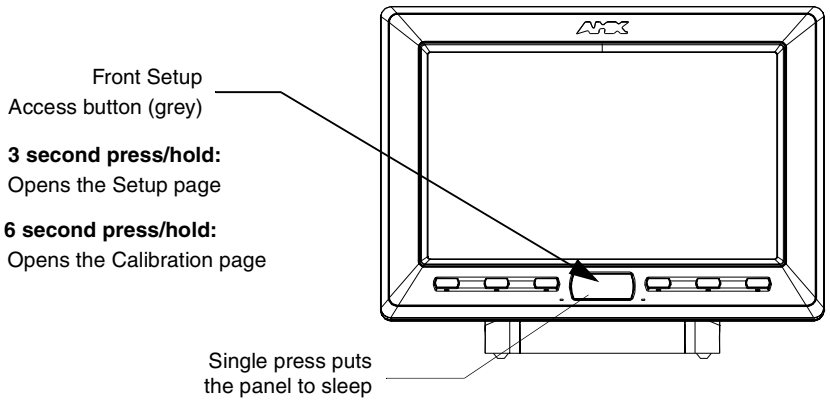


FIG. 48 Location of Front Setup Access button

2. Press the crosshairs (on the Calibration page) to set the calibration points on the LCD (FIG. 49).

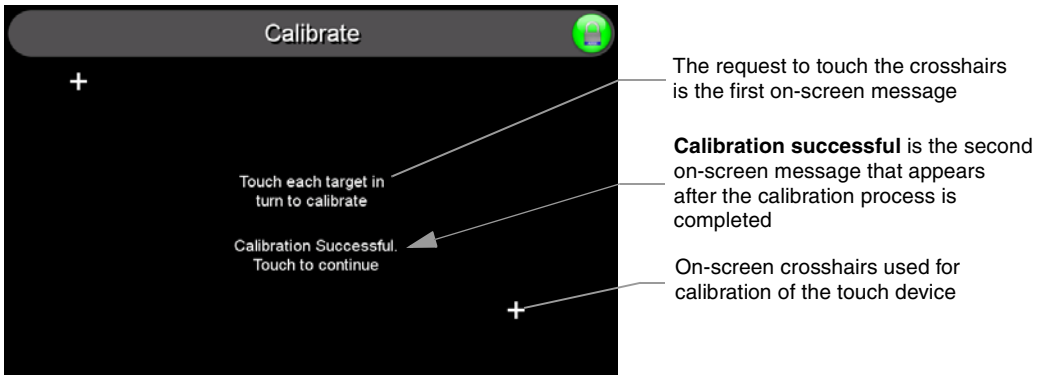

Calibrate
Touch each target in turn to calibrate
Calibration Successful. Touch to continue
The request to touch the crosshairs is the first on-screen message
Calibration successful is the second on-screen message that appears after the calibration process is completed
On-screen crosshairs used for calibration of the touch device

FIG. 49 Touch Panel Calibration Screens

3. After the "***Calibration Successful..***" message appears, press anywhere on the screen to continue and return to the Setup page.

NOTE

If the calibration was improperly set and you cannot return to the Calibration page (through the panel's firmware); *you can then access this firmware page via G4 WebControl where you can navigate to the Protected Setup page and press the Calibrate button through your VNC window.*
This action causes the panel to go to the Calibration page seen above, where you can physically recalibrate the actual touch panel again using the above procedures.

Testing your Calibration

1. Press and hold down the on-screen **Calibration** button for 6 seconds to enter the Calibration Test page (FIG. 50).

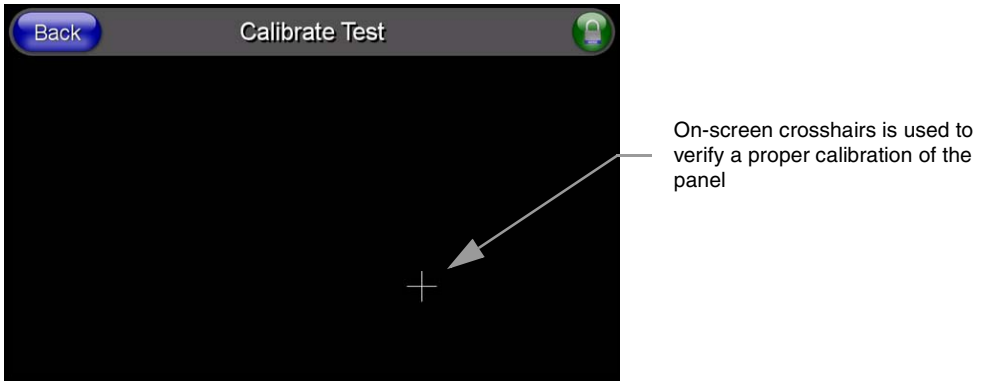


FIG. 50 Calibration Test page

2. Press anywhere on this page to confirm the on-screen crosshairs match your touch points.
3. If the crosshairs do not appear directly below your LCD touch points, press the **Back** button and recalibrate the panel using the above steps.
4. Exit this Calibration Test page by pressing the **Back** button to return to the Protected Setup page.

Configuring Communication

Communication between the Modero panel and the Master is done using either **USB** or **ETHERNET** (**DHCP or Static IP**). Ethernet communication can be achieved through either a direct connection (Ethernet) or through the use of the optional NXA-WC802.11GCF wireless CF card.

WARNING

Before commencing, verify you are using the latest NetLinx Master and Modero panel firmware. Verify you are using the latest versions of AMX's NetLinx Studio and TPDesign4 programs.

NOTE

USB input devices must be plugged into the rear or side USB connectors before the G4 panel is powered-up. The panel will not detect a USB connection of this type until after the unit cycles power.

Modero Setup and System Connection

1. Press the grey Front Setup Access button for **3 seconds** to open the Setup page (FIG. 51).

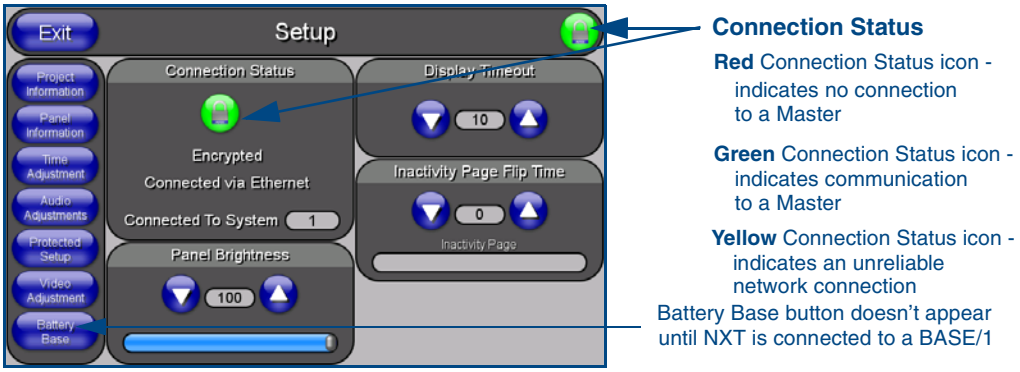


FIG. 51 Setup page

2. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
3. Enter ***1988*** into the Keypad's password field and press **Done** when finished.

NOTE

Clearing Password #5, from the initial Password Setup page, removes the need for you to enter the default password before accessing the Protected Setup page.

4. Press the red *Device Number* field to open the Device Number keypad (FIG. 52).
5. Enter a **Device Number** for the panel into the Device Number Keypad.
   The default is 10001 and the range is from 1 - 32000.

NOTE

When using multiple panels within a NetLinx System, remember to assign unique Device Number values to each panel so that all assigned panels appear in the System listing for the target Master.

6. Press **Done** to close the keypad, assign the number, and return to the Protected Setup page.
7. Press the on-screen **Reboot** button to restart the panel and incorporate any changes.

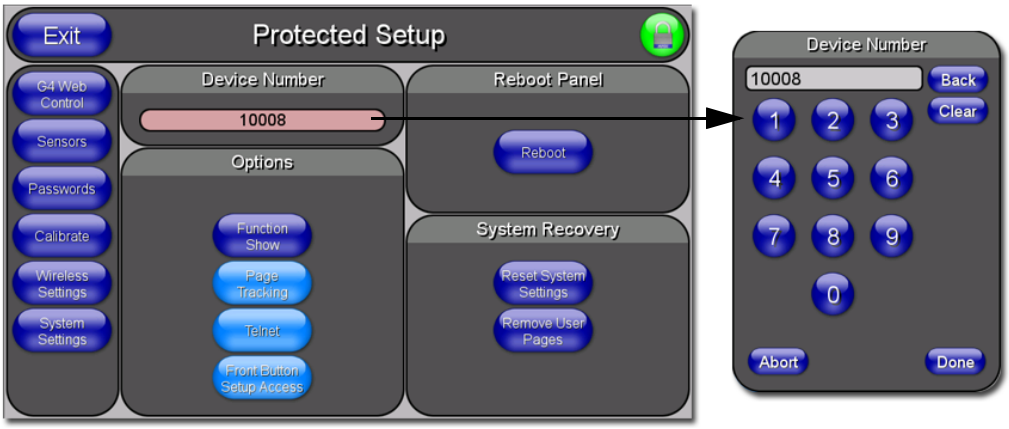


FIG. 52 Protected Setup page

Before continuing, open NetLinx Studio. This program assists in developing a System Number, Master IP/URL, and Master Port number. Refer to your NetLinx Master's instruction manuals for more information.

8. Obtain the System Number and Master IP Address from NetLinx Studio. This information must be specific for the system used with the configured Modero panel.
9. Press the grey Front Setup Access button for **3 seconds** to open the Setup page.
10. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page.
11. Press the **System Settings** button (located on the Protected Setup page) to open the System Settings page (FIG. 53) and begin configuring the communication settings on the panel to match those of the target Master.

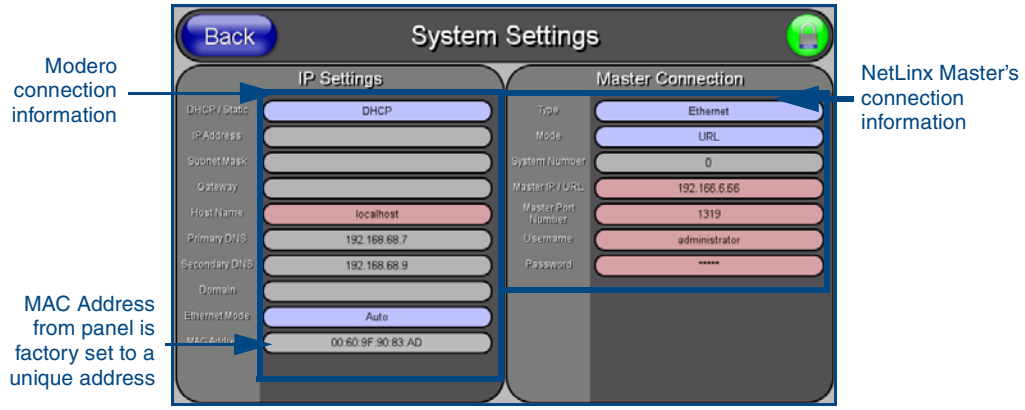


FIG. 53 System Settings page

*There are 2 possible Master Connection Types available: **USB** or **Ethernet**.*
*A USB connection type is a **direct connection** from the panel's mini-USB port to a corresponding USB port on the PC (acting as a Virtual Master).*
An Ethernet connection type involves indirect communication from the panel to a Master via an Ethernet connection to the network.

WARNING

It is recommended that firmware KIT files only be transferred over a direct connection and only when the panel is connected to a power supply. If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.

NOTE

*The mini-USB connector **MUST** be plugged into an already active panel before the PC can recognize the connection and assign an appropriate USB driver. This driver is part of both the NetLinx Studio and TPDesign4 software application installations.*

Configuring and Using USB with a Virtual Master

NetLinx Studio can be setup to run a Virtual Master where the PC acts as the Master by supplying its own IP Address for communication to the panel. The PC is first equipped with the USB driver, the panel is then configured for USB communication, and then Studio is configured to act as the Master.

For a personal computer to establish a connection to a Modero panel via USB, the target computer must have the appropriate AMX USB driver installed. This installation is bundled into the latest TPDesign4 software setup process or can be downloaded independently from the main Application Files page on **www.amx.com**.

Step 1: Setup the Panel and PC for USB Communication

1. If you do not currently have the latest version of TPDesign4, navigate to **www.amx.com > Tech Center > Downloadable Files > Application Files > NetLinx Design Tools** section of the website and locate the AMX USB Driver executable (**AMX USBLAN Setup exe**).
2. Download this executable file to a known location on your computer.
3. Launch the Setup.exe and follow the on-screen prompts to complete the installation.

Step 2: Confirm the Installation of the USB Driver on the PC

The first time each AMX touch panel is connected to the PC it is detected as a new hardware device and the USBLAN driver becomes associated with it (**panel specific**). Each time thereafter the panel is "recognized" as a unique USBLAN device and the association to the driver is done in the background. When the panel is detected for the **first time** some user intervention is required during the association between panel and driver.

1. After the installation of the USB driver has been completed, confirm the proper installation of the large Type-A USB connector to the PC's USB port, and restart your machine.

NOTE

If the panel is already powered, continue with steps 3.
The panel MUST be powered and configured for USB communication before connecting the mini-USB connector to the panel's Program Port.

2. Connect the terminal end of the 12 VDC-compliant power supply cable to the power connector on the rear/side of the touch panel and then apply power.
3. After the panel powers-up, press and hold the grey Front Setup Access button (**for 3 seconds**) to continue with the setup process and proceed to the Setup page.
4. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page (FIG. 54).
5. Toggle the blue *Type* field (***from the Master Connection section***) until the choice cycles to **USB**. Refer to the *System Settings Page* section on page 132 for more information about the fields on this page.

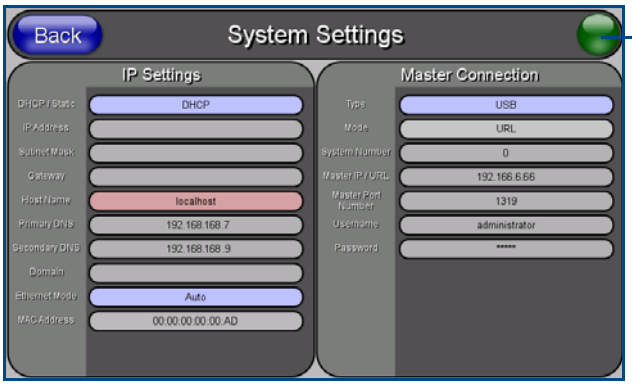


FIG. 54 USB System Settings page - using a USB Connection Type

NOTE

***ALL** fields are then greyed-out and read-only, but still display any previous network information.*

6. Press the **Back** button on the touch panel to return to the Protected Setup page.
7. Press the on-screen **Reboot** button to both save any changes and **restart the panel.** *Remember that the panel's connection type must be set to **USB** prior to rebooting the panel and prior to inserting the USB connector.*
8. **ONLY AFTER** the unit displays the first panel page, **THEN** insert the mini-USB connector into the Program Port on the panel. It may take a minute for the panel to detect the new connection and send a signal to the PC (*indicated by a green System Connection icon*). If this is your first time installing the USB driver, a USB driver installation popup window (FIG. 55) appears on the PC.

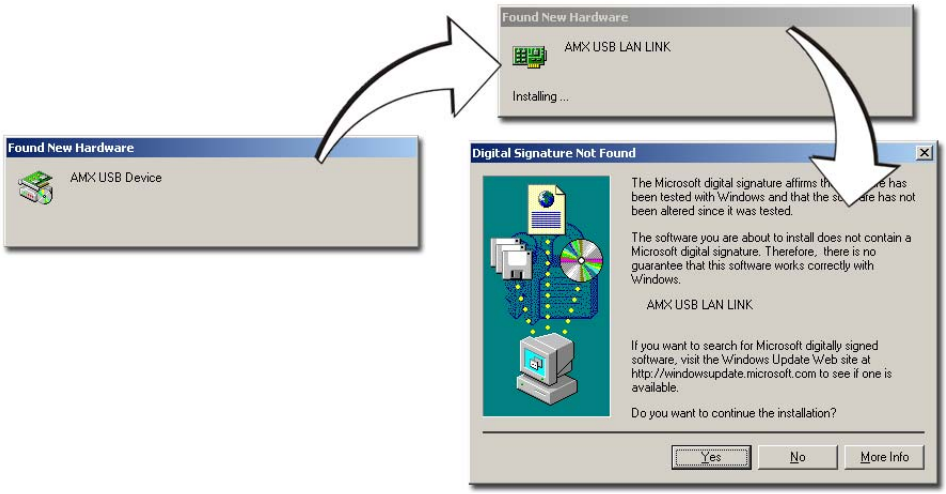

Found New Hardware
AMX USB LAN LINK
Installing ...
Found New Hardware
AMX USB Device
Digital Signature Not Found
The Microsoft digital signature affirms th has been tested with Windows and that the s has not been altered since it was tested.
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.
AMX USB LAN LINK
If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.
Do you want to continue the installation?
Yes
No
More Info

FIG. 55 USB driver installation popup window

- This window notifies you that the panel has been detected by the PC as a USB-compliant device and the PC is installing an appropriate USB driver to establish a proper communication to the panel.
- This driver was installed on your PC during the installation of the latest NetLinx Studio and TPDesign4 software application installations. **These applications should be installed prior to setting up a USB connection to the panel.**

- The driver does not contain a Microsoft® digital signature and Windows® then informs you of such.

9. Click **Yes** when told that a digital signature was not found. This action accepts the installation of the new AMX USB driver. **The panel is now configured to communicate directly with the PC.**
   - This process completes the association between driver and device.
     Each time the same touch panel is connected to the computer the driver is automatically loaded (*using a unique name - example USB LAN LINK #1, #2*).
     Each time a different touch panel is connected to the computer, the previous procedures will need to be repeated.
10. Navigate back to the System Settings page.

Step 3: Confirm and View the current AMX USB device connections

The USB driver information can be confirmed via two different methods:

- Via the Control panel (previous steps 1 and 2) or
- Via the **Unplug or Eject Hardware** icon from the Taskbar.

1. Navigate to **Start > Settings > Control Panel >** and double-click the **System** icon to launch the System Properties dialog.
2. Select the **Hardware** tab and click on the **Device Manager** button to launch the Device Manager dialog.
   - Within the *Device Manager* dialog, the AMX USBLAN device appears under Network Adapters (FIG. 56) and has a unique name such as AMX USB LAN LINK #2. The number changes depending on which recognized panel is currently connected.

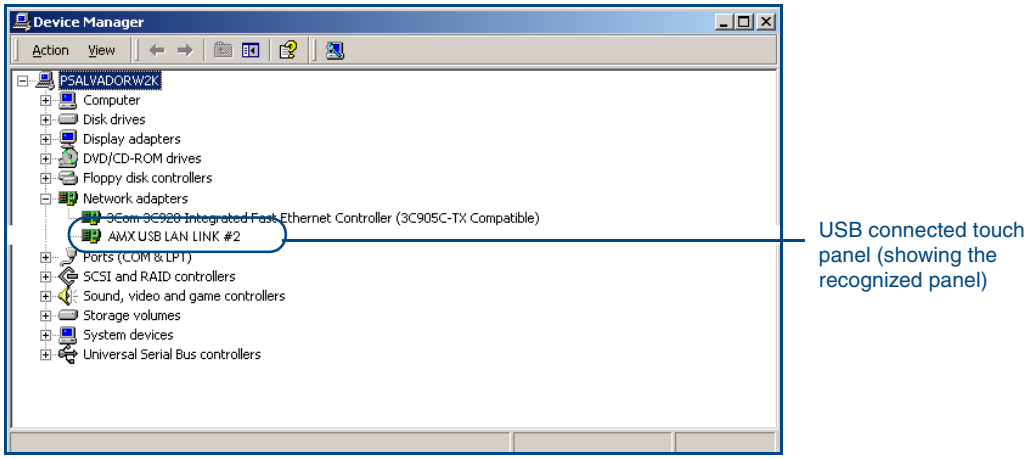


FIG. 56 Device Manager dialog showing USB device

3. Confirm that a new USB detection icon (FIG. 57) appears in the lower-right taskbar on the PC display window.
4. Double-click on the icon to open the **Unplug or Eject Hardware** window and confirm the AMX USB LAN LINK has been installed and is operating properly.

NOTE

A Virtual NetLinx Master (VNM) is used when the target panel is not connected to a physical NetLinx Master. In this situation, the PC takes on the functions of a Master via a Virtual NetLinx Master. ***This connection is made by either using the PC's Ethernet Address (via TCP/IP using a known PC's IP Address as the Master) or using a direct mini-USB connection to communicate directly to the panel****.*

5. Click the **Properties** button to view further information about the installed USB driver.

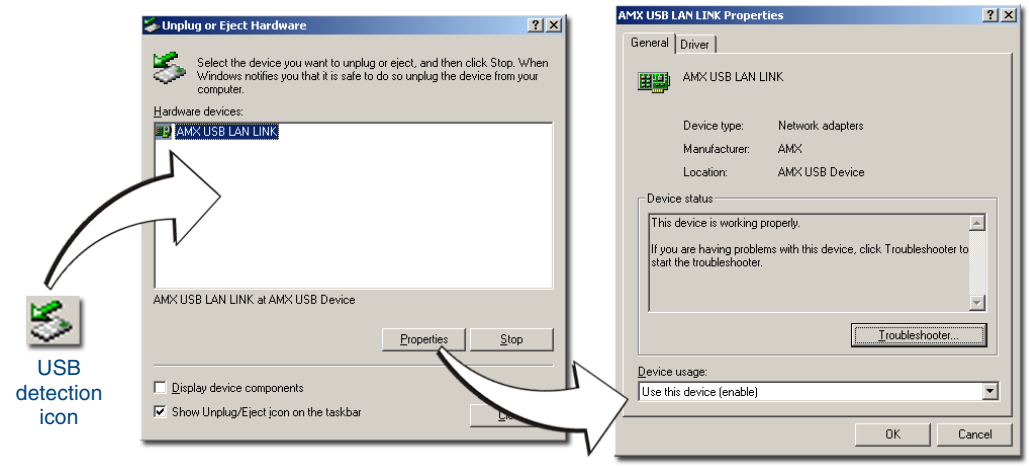

Unplug or Eject Hardware
Select the device you want to unplug or eject, and then click Stop. When Windows notifies you that it is safe to do so unplug the device from your computer.
Hardware devices:
AMX USB LAN LINK
AMX USB LAN LINK at AMX USB Device
Properties
Stop
Display device components
Show Unplug/Eject icon on the taskbar
USB detection icon
AMX USB LAN LINK Properties
General
Driver
AMX USB LAN LINK
Device type: Network adapters
Manufacturer: AMX
Location: AMX USB Device
Device status
This device is working properly.
If you are having problems with this device, click Troubleshooter to start the troubleshooter.
Troubleshooter...
Device usage:
Use this device (enable)
OK
Cancel

FIG. 57 USB Properties windows

NOTE

If there is a yellow exclamation point next to the AMX USB LAN LINK device (within the hardware devices section of the Unplug or Eject Hardware window), stop and close the USB operation. Reconnect the USB cable to the panel and repeat the setup procedures. Refer to the Troubleshooting section on page 185 *for more detailed information.*

To remove the USB driver association from a previously connected touch panel, you must navigate back to the Device Manager, right-click on the panel's USB driver (example AMX USB LAN LINK #2) and select **Uninstall** from the context menu and then **OK**.

- Once the system completes the removal of the device, the Device Manager window will refresh, and the device will no longer appear.
- The next time this device is connected to the computer it will appear as a new hardware device and will need to be associated again with the driver (refer to *Step 2: Confirm the Installation of the USB Driver on the PC* section on page 53.

Step 4: Use the USB to Configure a Virtual Master (using NetLinx Studio)

NOTE

*When configuring your panel to communicate via USB with a Virtual Master (on your PC), ONLY the **USB** connection option must be selected within the Type field. Since this is a direct connection, the PC's IP Address is not needed.*

Before beginning:

1. Verify the panel has been configured to communicate via USB within the System Settings page and that the USB driver has been properly configured. Refer to the previous section for more information.
2. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
3. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 58).
4. Click the **Communications Settings** button to open the *Communications Settings* dialog.
5. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.

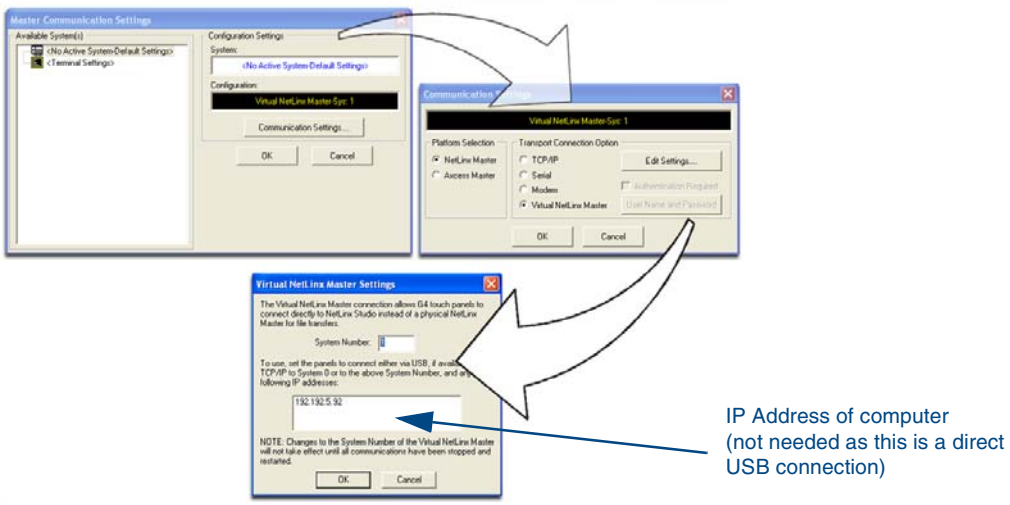


FIG. 58 Assigning Communication Settings for a Virtual Master

6. Click on the **Virtual Master** radio box (*from the Transport Connection Option section*) to indicate you are wanting to configure the PC to communicate directly with a panel. Everything else such as the Authentication is greyed-out because you are not going through the Master's UI.
7. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the *Virtual NetLinx Master Settings* dialog (FIG. 58).
8. From within this dialog enter the System number (default is **1**).
9. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
10. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is one*.
11. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list.
    The panel will not appear as a device below the virtual system number (in the Online Tree tab) until both the system number used in step 8 for the VNM is entered into the Master Connection section of the System Settings page and the panel is restarted.
    - The Connection status turns green after a few seconds to indicate an active USB connection to the PC (Virtual Master). No Lock icon is displayed because this USB connection is not secured (*requiring a username/password*).

NOTE

If the G4 panel does not appear, refer to the Troubleshooting section on page 185 *for more information.*

- If a few minutes have gone by and the System Connection icon still does not turn green, repeat the USB connection and Virtual Master setup procedures (outlined in this section). Refreshing the System sends out a request to the panel to respond and completes the communication (*turning the System Connection icon green*).

Step 5: Confirm and View the current AMX USB device connections

Use the CC-USB Type-A to Mini-B 5-wire programming cable (**FG10-5965**) to provide communication between the mini-USB Program port on the touch panel and the PC. This method of communication is used to transfer firmware KIT files and TPD4 touch panel files.

NOTE

A mini-USB connection is only detected after it is installed onto an active panel. Connection to a previously powered panel which then reboots, allows the PC to detect the panel and assign an appropriate USB driver.

1. Verify this direct USB connection (Type-A on the panel to mini-USB on the panel) is configured properly using the steps outlined in the previous two sections.
2. With the panel already configured for USB communication and the Virtual Master setup within NetLinx Studio, its now time to verify the panel is ready to receive files.
3. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is one*.
4. Right-click on the System entry (**A** in FIG. 59) and select **Refresh System**. This causes a refresh of all project systems, establishes a new connection to the Virtual Master, and populates the System list with devices on your particular system.

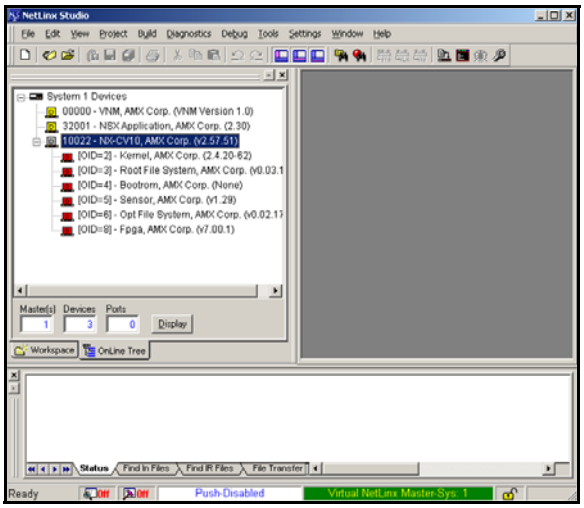

NetLinx Studio
File Edit View Project Build Diagnostics Debug Tools Settings Window Help
System 1 Devices
00000 - VNM, AMX Corp. (VNM Version 1.0)
32001 - NSX Application, AMX Corp. (2.30)
10022 - NX-CV10, AMX Corp. (v2.57.51)
[OID=2] - Kernel, AMX Corp. (2.4.20-62)
[OID=3] - Root File System, AMX Corp. (v0.03.1
[OID=4] - Bootrom, AMX Corp. (None)
[OID=5] - Sensor, AMX Corp. (v1.29)
[OID=6] - Opt File System, AMX Corp. (v0.02.17
[OID=8] - Fpga, AMX Corp. (v7.00.1)
Master(s) Devices Ports
Display
Workspace
OnLine Tree
Status
Find In Files
Find IR Files
File Transfer
Ready
Push-Disabled
Virtual NetLinx Master-Sys: 1

FIG. 59 Using USB for Virtual Master communication

Wireless Settings Page - Wireless Access Overview

IP Routing

The behavior of the wireless routing is largely dependent on the wired network interface. Although the panel can be connected to two networks simultaneously it may only have one gateway. If the wired network was successfully set up and a gateway was obtained; then the default route for all network traffic will be via the wired network. In the event that the wired network was not configured, then the default route for all network traffic will be via the wireless network. The wired network connection always takes priority.

As an example:

- Imagine a panel connected to two networks A & B. **A** is the wired network and **B** is the wireless network. If the Master controller is on either of these networks then it will be reached. However if the Master controller is on a different network, **C**, then determining which network interface (wired or wireless) that will be used is dependent on the gateway.

Hot Swapping

Hot swapping is not an issue on these panels as the card is installed within the unit and cannot be removed without first removing the housing.

In the case of DHCP, there must be a DHCP server accessible before the fields are populated.

If the SSID (Network Name) and WEP fields have not previously been configured, the Wireless Settings page will not work until the panel is rebooted.

Ethernet Communication from the panel can be direct (using an Ethernet cable) or indirect (through the NXA-WC80211GCF AMX Wireless Card communicating to a Wireless Access Point (WAP) such as the NXA-WAP200G). **The Wireless Access Point communication parameters must match those of the installed wireless CF card inside the panel.**

In determining the Ethernet method of communication, the panel will always default first to the direct Ethernet communication. If no direct connection is detected, the panel will first check to see if there is an installed wireless interface card and then communicate to the WAP using the Wireless Settings assigned within the Wireless Settings page. The WAP communication parameters must match those of the pre-installed wireless interface card installed within the panel. These touch panels allow users to connect to a wireless network through their use of the optional AMX 802.11g Wi-Fi CF card. The WAP communication parameters must match those of the pre-installed wireless interface card installed within the panel. This internal card transmits data wirelessly using the 802.11x signals at 2.4 GHz.

For a more detailed explanation of the new security and encryption technology, refer to the section of the document entitled: *Appendix B - Wireless Technology* section on page 197.

Configuring a Wireless Connection

When working with a wireless card, the first step is to configure wireless communication parameters within the Wireless Settings page. This page only configures the card to communicate to a target WAP (such as the NXA-WAP200G), **it is still necessary to tell the panel which Master it should be communicating with**. This "pointing to a Master" is done via the System Settings page where you configure the IP Address, System Number and Username/Password information assigned to the target Master.

Step 1: Configure the Panel's Wireless IP Settings

The first step to successfully setting up your internal wireless card is to configure the IP Settings section on the Wireless Settings page. The section configures the communication parameters from the Modero panel to the web.

Wireless communication using a DHCP Address

1. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
2. Enter ***1988*** into the Keypad's password field and press **Done** when finished.
3. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page. Wireless communication is set within the IP Settings section of this page (FIG. 60).
4. Toggle the *DHCP/Static* field (***from the IP Settings section***) until the choice cycles to **DHCP**. *This action causes all fields in the IP Settings section (other than Host Name) to be greyed-out.*

NOTE

DHCP will register the unique MAC Address (factory assigned) on the panel and once the communication setup process is complete, assign IP Address, Subnet Mask, and Gateway values from the DHCP Server.

5. Press the optional *Host Name* field to open a Keyboard and enter the Host Name information.

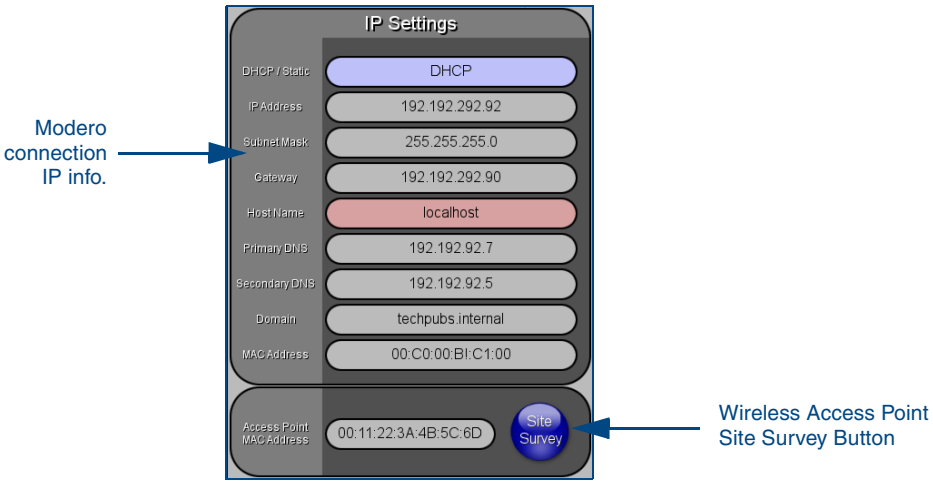


FIG. 60 Wireless Settings page (IP Settings section)

6. Press **Done** after you are finished assigning the alpha-numeric string of the host name.
7. Do not alter any of these remaining greyed-out fields in the IP Settings section. Once the panel is rebooted, these values are obtained by the unit and displayed in the *DNS* fields after power-up.

NOTE

This information can be found in either the Workspace - System name > Define Device section of your code (that defines the properties for your panel), or in the Device Addressing/Network Addresses section of the Tools > NetLinx Diagnostics dialog.

8. Setup the security and communication parameters between the wireless card and the target WAP by configuring the Wireless Settings section on this page. Refer to *Step 2: Configure the Card's Wireless Security Settings* section on page 63 for detailed procedures to setup either a secure or insecure connection.

Wireless communication using a Static IP Address

1. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
2. Enter ***1988*** into the Keypad's password field and press **Done** when finished.
3. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page. Wireless communication is set within the IP Settings section of this page (FIG. 60).

Check with your System Administrator for a pre-reserved Static IP Address assigned to the panel. This address must be obtained before Static assignment of the panel continues.

4. Toggle the *DHCP/Static* field (***from the IP Settings section***) until the choice cycles to **Static**. *The IP Address, Subnet Mask, and Gateway fields then become user-editable (red).*
5. Press the *IP Address* field to open a Keyboard and enter the Static IP Address (*provided by your System Administrator*).
6. Press **Done** after you are finished entering the IP information.
7. Repeat the same process for the *Subnet Mask* and *Gateway* fields.
8. Press the optional *Host Name* field to open the Keyboard and enter the Host Name information.
9. Press **Done** after you are finished assigning the alpha-numeric string of the host name.
10. Press the Primary DNS field to open a Keyboard, enter the Primary DNS Address (provided by your System Administrator) and press **Done** when compete. Repeat this process for the Secondary DNS field.
11. Press the Domain field to open a Keyboard, enter the resolvable domain Address (this is provided by your System Administrator and equates to a unique Internet name for the panel), and press **Done** when complete.
12. Setup the security and communication parameters between the wireless card and the target WAP by configuring the Wireless Settings section on this page. Refer to the following section for detailed procedures to setup either a secure or insecure connection.

Using the Site Survey tool

This tool allows a user to "sniff-out" all transmitting Wireless Access Points within the detection range of the internal NXA-WC80211GCF (***this feature is not available with the 802.11b Wi-Fi card***). Once pressed, the panel displays the Site Survey page which contains categories such as:

- **Network Name** (SSID) - Wireless Access Point names
- **Channel** (RF) - Channel currently being used by the WAP (*Wireless Access Point*)
- **Security Type** (if detectable - such as **WEP**, **OPEN** and **UNKNOWN**) - security protocol enabled on the WAP
- **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent
- **MAC Address** - Unique identification of the transmitting Access Point

1. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page.
2. Navigate to the Access Point MAC Address section of this page and press the on-screen **Site Survey** button. This action launches the Site Survey page which displays a listing of all detected WAPs in the communication range of the internal card.
   - The card scans its environment every four seconds and adds any new WAPs found to the list. Every scan cycle updates the signal strength field.

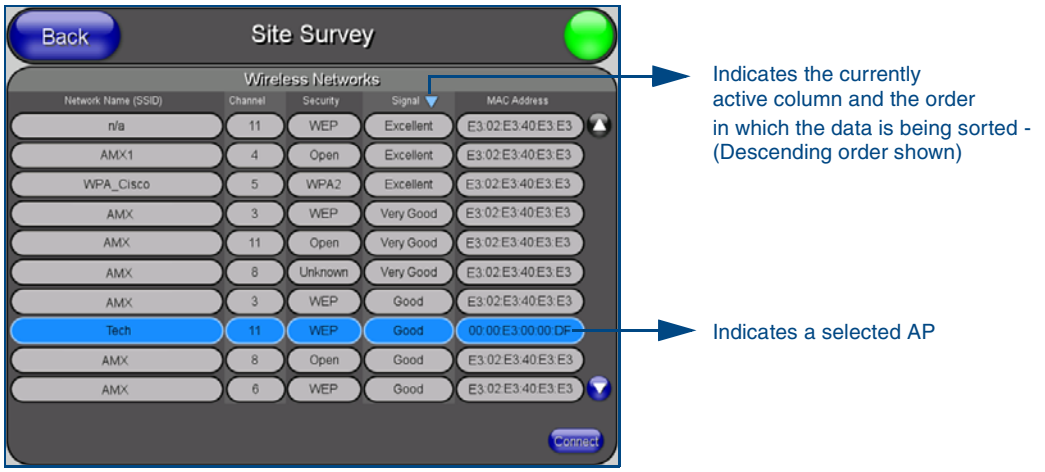

Back
Site Survey
Wireless Networks
Network Name (SSID)
Channel
Security
Signal
MAC Address
n/a 11 WEP Excellent E3:02:E3:40:E3:E3
AMX1 4 Open Excellent E3:02:E3:40:E3:E3
WPA_Cisco 5 WPA2 Excellent E3:02:E3:40:E3:E3
AMX 3 WEP Very Good E3:02:E3:40:E3:E3
AMX 11 Open Very Good E3:02:E3:40:E3:E3
AMX 8 Unknown Very Good E3:02:E3:40:E3:E3
AMX 3 WEP Good E3:02:E3:40:E3:E3
Tech 11 WEP Good 00:00:E3:00:00:DF
AMX 8 Open Good E3:02:E3:40:E3:E3
AMX 6 WEP Good E3:02:E3:40:E3:E3
Connect
Indicates the currently active column and the order in which the data is being sorted - (Descending order shown)
Indicates a selected AP

FIG. 61 Site Survey page

- Access points are tracked by MAC Address.
  - If the WAP's SSID is set as a blank, then **N/A** is displayed within the *SSID* field.
  - If the WAP's SSID is hidden (*not broadcast*) it will not show up on the site survey screen but it can still be configured via the *SSID* field on the specified security mode screen.
  - If a WAP is displayed in the list is not detected for 10 scans in a row it is then removed from the screen. In this way, a user can walk around a building and see access points come and go as they move in and out of range.

3. Sort the information provided on this page by pressing on a column name and toggling the direction of the adjacent arrow.
   - **Up arrow** - indicates that the information is being sorted in a Ascending order.
     - **SSID** (A to Z), **Channel** (1 to 14), **Security** (Unknown to WEP), **Signal** (None to Excellent). The firmware considers the following to be the security order from least secure to most secure: Open, WEP, WPA, WPA2, and Unknown.
   - **Down arrow** - indicates that the information is being sorted in a Descending order.
     - **SSID** (Z to A), **Channel** (11 to 6), **Security** (WEP to Unknown), **Signal** (Excellent to None)

NOTE

If the panel detects more than 10 WAPs, the Up/Down arrows at the far right side of the page become active (blue) and allow the user to scroll through the list of entries.

4. Select a desired Access Point by touching the corresponding row. The up arrow and down arrow will be grayed out if there are ten or less access points detected. If there are more, then they will be enabled as appropriate so that the user can scroll through the list.
5. With the desired WAP selected and highlighted, click the **Connect** button to be directed to the selected security mode's Settings page with the *SSID* field filled in. You can then either **Cancel** the operation or fill in any necessary information fields and then click **Save**.
   *If you select an Open, WEP, and WPA-PSK Access Point and then click **Connect**, you will be flipped to the corresponding Settings page. For any other security mode, if you click **Connect** you will only return to the previous page without any information being pre-filled out for you.*
   - In an Open security mode, when a target WAP is selected and the connect to, the SSID name of the selected WAP is saved for the open security mode.

- In a Static WEP security mode, when a WEP Access Point is selected and then connected to, the user is then redirected back to the Static WEP security screen where the *SSID* field is already filled out and the user is only required to enter in the remaining WEP key settings.
- A similar process occurs for WPA-PSK access points. For any other case, the firmware switches back to the previous page and security and connection parameters must be entered in as normal.

Step 2: Configure the Card's Wireless Security Settings

The second step to successfully setting up your wireless card is to configure the Wireless Settings section of the Wireless Settings page. The section configures both the communication and security parameters from the internal wireless card to the WAP. ***The procedures outlined within the following sections use an 802.11g card to configure a common security configuration to a target WAP.***

NOTE

Once you have completed setting up the wireless card parameters, you must then navigate to the System Settings page and configure the communication parameters for the target Master. Until those parameters are configured, your Connection Status icon will remain red (indicating that there is no current connection to a Master).

Configuring the Modero's wireless card for unsecured access to a WAP200G

NOTE

Prior to beginning the configuration of the wireless settings, verify that the panel has been upgraded to a wireless panel via the installation of the NXA-WC80211GCF wireless CF card.

1. Power-down the panel and follow the wireless card installation procedures outlined in the *Installation and Upgrade of the Internal NXT Components* section on page 21 and *Installation and Upgrade of the Internal NXD Components* section on page 26.
2. Power-up the panel (this allows it to detect the card).
3. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
4. Enter ***1988*** into the Keypad's password field and press **Done** when finished.
5. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page.

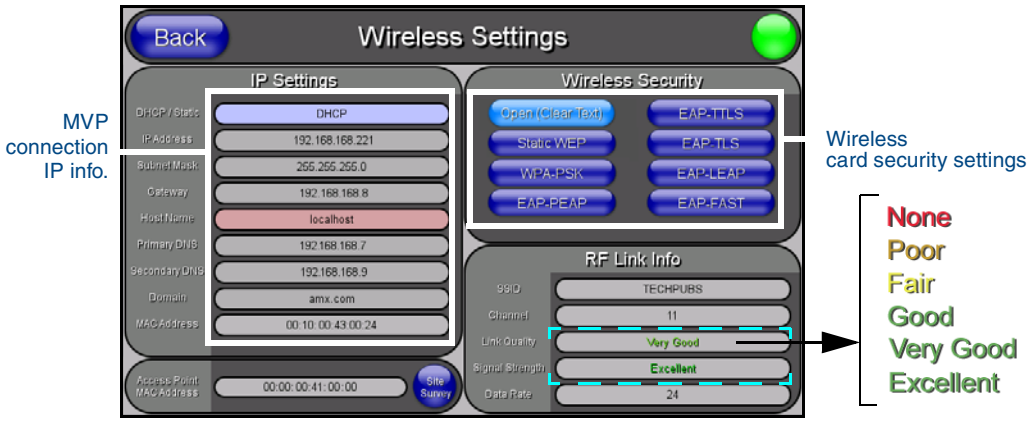


FIG. 62 Wireless Settings page (showing a sample unsecured configuration)

6. Enter the SSID information by either:

- *Automatically* having it filled in by pressing the Site Survey button and from the Site Survey page, choosing an ***Open*** WAP from within the Site Survey page and then pressing the **Connec**t button.

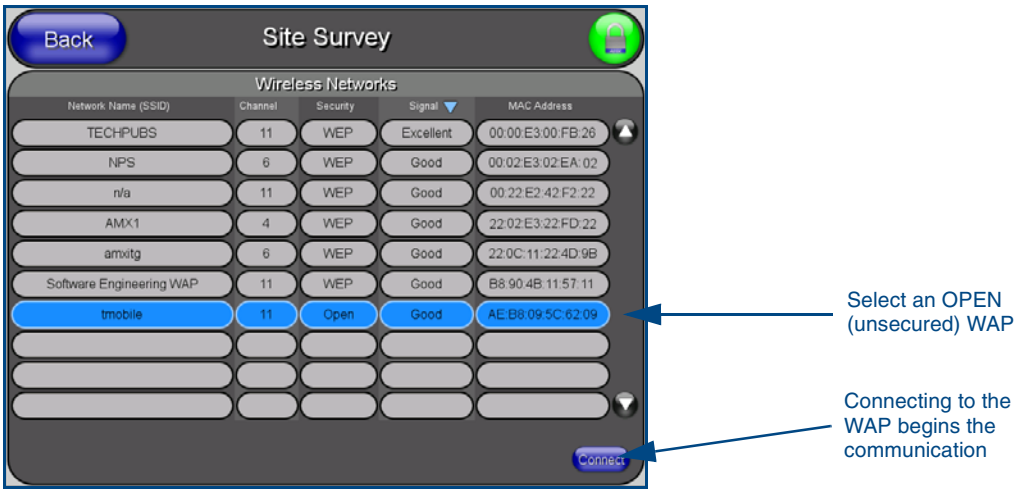


FIG. 63 Site Survey of available WAPS (Unsecured WAP shown selected)

- *Manually* entering the SSID information into their appropriate fields by following steps 7 thru 9.

7. From within the Wireless Security section, press the **Open (Clear Text)** button to open the Open (Clear Text) Settings dialog (FIG. 64). An Open security method does not utilize any encryption methodology but does require that an SSID (alpha-numeric) be entered. Using this method causes network packets to be sent out as unencrypted text.

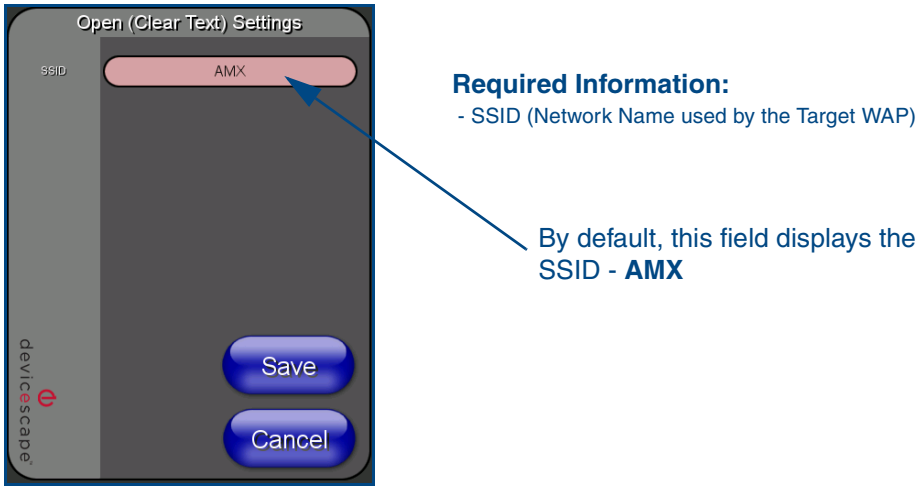


FIG. 64 Wireless Settings page - Open (Clear Text) security method

8. Press the red *SSID* field (FIG. 64) to display an on-screen *Network Name (SSID)* keyboard.

9. In this keyboard, enter the SSID name used on your target Wireless Access Point (**case sensitive**).

- The card should be given the SSID used by the target WAP. If this field is left blank, the unit will attempt to connect to the first available WAP. By default, all WAP200Gs use **AMX** as their assigned SSID value.

- One of the most common problems associated with connection to a WAP arise because the SSID was not entered properly. You must maintain the same case when entering the SSID information. ABC is not the same as Abc.

10. Click **Done** when you've completed typing in the information.
11. From the Open (Clear Text) Settings page (FIG. 64), press the **Save** button to incorporate your new information into the panel and begin the communication process.
12. Verify the fields in the *IP Settings* section have been properly configured. Refer to *Step 1: Configure the Panel's Wireless IP Settings* section on page 60 for detailed information.
13. Press the **Back** button to return to the Protected Setup page and press the on-screen **Reboot** button to both save any changes and restart the panel. ***Remember that you will need to navigate to the System Settings page and configure the connection to a target Master.***
14. After the panel restarts, return to the Wireless Settings page's RF Link Info section and verify the Link Quality and Signal Strength:
    - The descriptions are: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent** (FIG. 64).

The signal strength field should provide some descriptive text regarding the strength of the connection to a Wireless Access Point. If there is no signal or no IP Address displayed; configuration of your network could be required.

Configuring the Modero's wireless card for secured access to a WAP200G

After logging into the WAP200G, the default Status page appears within the web browser. These read-only values are "pulled" from some of the other user-configurable Configuration Utility pages. By default, wireless Modero panels are configured for unsecured communication to a Wireless Access Point. To properly setup both the WAP200G and panel for secure communication, you must first prepare the Modero panel and then use the information provided to fill out the fields within the WAP's browser-based Basic Wireless Configuration page.

Since the code key generator on Modero panels use the same key generation formula, all panels will generate identical keys for the same Passphrase. The generators used on WAPs will not produce the same key as the Modero generator even if you use the same Passphrase. **For this reason, we recommend FIRST creating the Current Key on the Modero and then entering that information into the appropriate NXA-WAP200G fields**.

1. Provide power to the panel (this allows it to detect the internal wireless card).
2. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
3. Enter ***1988*** into the Keypad's password field and press **Done** when finished.
4. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page.
5. Locate the Wireless Security section (FIG. 65).

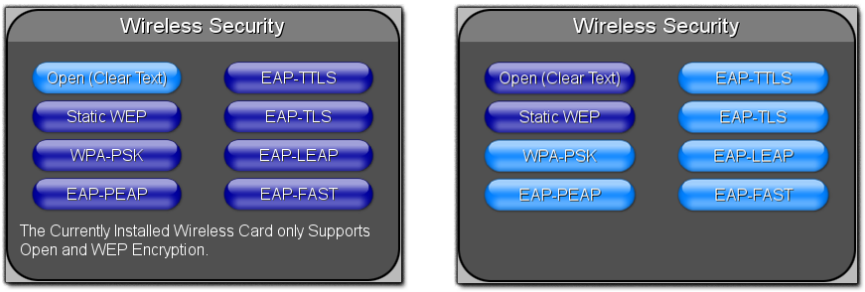
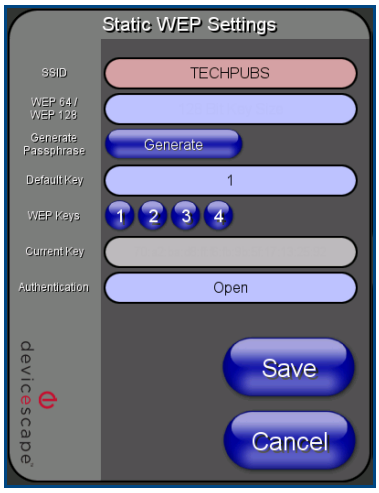


FIG. 65 Wireless Settings page (showing how each card supports its own security features)

NOTE

You must first take down the SSID name, Current Key string value, and panel MAC Address information so you can later enter it into the appropriate WAP dialog fields in order to "sync-up" the secure connection. These values must be identically reproduced on the target WAP.

6. Press the **Static WEP** button to open the Static WEP Settings dialog (FIG. 66).



Required Information:
- SSID (Network Name used by the Target WAP)
- Encryption Method
- Passphrase
- WEP Key assignment
- Authentication Method

FIG. 66 Wireless Settings page - Static WEP security method

7. Enter the SSID information by either:
   - *Automatically* having it filled in by pressing the **Site Survey** button, navigating to the Site Survey page, choosing a ***WEP*** secured WAP from within the Site Survey page, and then pressing the **Connect** button.
   - *Manually* entering the SSID information into the appropriate field by following step 8.
8. Press the *SSID* field and from the *Network Name (SSID)* keyboard, enter the SSID name you are using on your target Wireless Access Point (**case sensitive**), and press **Done** when finished.
   - The card should be given the SSID used by the target WAP. If this field is left blank, the unit will attempt to connect to the first available WAP. By default, all WAP200Gs use **AMX** as their assigned SSID value.
   - One of the most common problems associated with connection to a WAP arise because the SSID was not entered properly. You must maintain the same case when entering this information. ***ABC is not the same as Abc***.

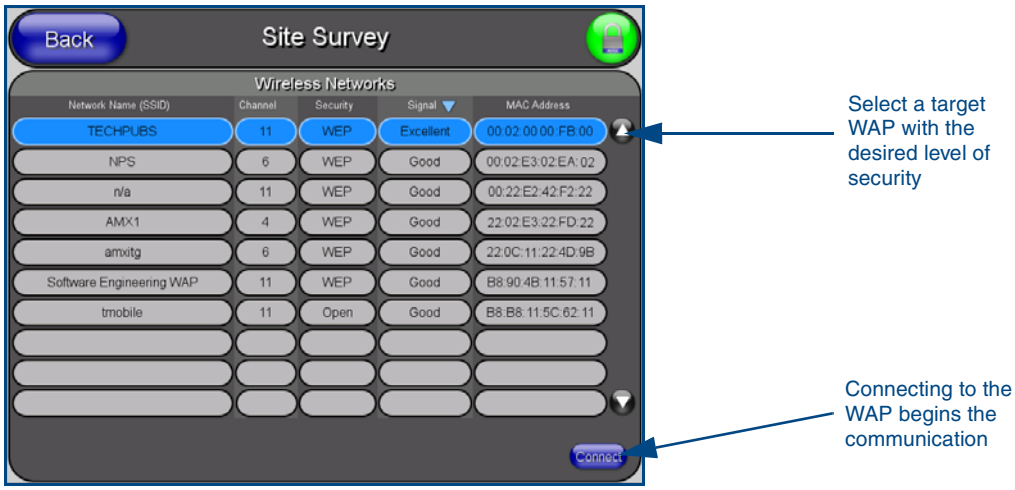


FIG. 67 Site Survey of available WAPs (Secured WAP shown selected)

- The alpha-numeric string is by default **AMX** but can later be changed to any 32-character entry. *This string must be duplicated within the Network Name (SSID) field on the WAP.*
- As an example, if you use **TECHPUBS** as your SSID, you must **match this word and the case** within both the *Network Name (SSID)* field on the touch panel's *Network Name SSID* field and on the WAP's *Basic Wireless Configuration* page.

9. Toggle the *Encryption* field (FIG. 66) until it reads either: **64 Bit Key Size** or **128 Bit Key Size**. *The 64/128 selection reflects the bit-level of encryption security. This WEP encryption level must match the encryption level being used on the WAP.*

NOTE

WEP will not work unless the same Default Key is set on both the panel and the Wireless Access Point.
For example: if you have your Wireless Access Point set to default key 4 (which was 01:02:03:04:05), you must set the panel's key 4 to 01:02:03:04:05.

10. Toggle the *Default Key* field until the you've chosen a WEP Key value (**from 1- 4**) that matches what you'll be using on your target WAP200G. **This value MUST MATCH on both devices**.

- **These WEP Key identifier values must match for both devices.**

11. With the proper WEP Key value displayed, press the **Generate** button to launch the WEP Passphrase keyboard.
If you are wanting to have your target WAP (other than an NXA-WAP200G) generate the Current Key - Do not press the Generate button and continue with Step 13.

- This keyboard allows you to enter a Passphrase (such as *AMXPanel*) and then AUTOMATICALLY generate a WEP key which is compatible only among all Modero panels.

NOTE

The code key generator on Modero panels use the same key generation formula. Therefore, this same Passphrase generates identical keys when done on any Modero because they all use the same Modero-specific generator. The Passphrase generator is case sensitive.

12. Within this on-screen WEP Passphrase keyboard (FIG. 68), enter a character string or word (such as ***AMXPanel***) and press **Done** when you have finished.

FIG. 68 WEP Passphrase Keyboard

- As an example, enter the word **AMXPanel** using a 128-bit hex digit encryption. After pressing **Done**, the on-screen Current Key field displays a long string of characters (separated by colons) which represents the encryption key equivalent to the word AMXPanel.
- **This series of hex digits (26 hex digits for a 128-bit encryption key) should be entered as the *Current Key* into both the WAP and onto other communicating Modero panels by using the WEP Key dialog** (FIG. 69).

FIG. 69 WEP Key # Keyboard

13. Write down this Current Key string value for later entry into your WAP's *WEP Key* field (*typically entered without colons*) and into other communicating panel's *Current Key* field (FIG. 66).
14. **If you are entering a Current Key generated either by your target WAP or another Modero panel**, within the *WEP Keys* section, touch the **Key #** button to launch the *WEP Key #* keyboard (FIG. 69), enter the characters and press **Done** when finished.
    - This Key value corresponds to the Default WEP Key number used on the Wireless Access Point and selected in the Default Key field described in the previous step.

NOTE

If your target Wireless Access Point does not support passphrase key generation and has previously been setup with a manually entered WEP KEY, you must manually enter that same WEP key on your panel.

15. The remaining *Current Key* and *Authentication* fields are greyed-out and cannot be altered by the user.
16. Verify the fields within the IP Settings section have been properly configured. Refer to *Step 1: Configure the Panel's Wireless IP Settings* section on page 60 for detailed information.

17. Press the **Back** button to navigate to the Protected Setup page and press the on-screen **Reboot** button to both save any changes and restart the panel. ***Remember that you will need to navigate to the System Settings page and configure the connection to a target Master.***
18. After the panel restarts, return to the Wireless Settings page to verify the Link Quality and Signal Strength:
    - The descriptions are: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent**.

The signal strength field provides some descriptive text regarding the strength of the connection to a Wireless Access Point. If there is no signal or no IP Address displayed; configuration of your network could be required.

Refer to the NXA-WAP200G Instruction Manual for more detailed setup and configuration procedures.

Configuring multiple wireless Moderos to communicate to a target WAP200G

1. For each communicating touch panel, complete all of the steps outlined within the previous *Configuring the Modero's wireless card for secured access to a WAP200G* section on page 65.
    - Those procedures walk you through assigning an SSID, selecting a WEP encryption level, and obtaining a Current Key string value for a specific WEP Key on a target panel.
2. Navigate back to the Wireless/Wireless Settings page on each panel.
3. Verify that all communicating Modero panels are using the same **SSID**, **encryption level**, **Default Key #**, and an identical **Current Key value**.
    - As an example, all panels should be set to Default Key **#1** and be using **aa:bb:cc**..as the Current Key string value. This same Key value and Current Key string should be used on the target WAP.
4. Repeat steps 1 - 3 on each panel. **Using the same passphrase, generates the same key for all communicating Modero panels.**

Configuring a Wired Ethernet Connection

It is necessary to tell the panel which Master it should be communicating with. This "pointing to a Master" is done via the System Settings page where you configure the IP Address, System Number and Username/Password information assigned to the target Master. If you have previously established a wireless connection to the Internet you must still navigate to the System Settings page and configure the communication parameters for the target Master. Until those parameters are configured, your Connection Status icon will remain red (*indicating there is no current connection to a Master*).

- If you have previously configured an internal wireless card for communication to the Internet, you do not need to configure the panel's IP Settings fields and can skip the following Step 1.

Step1: Configure the Panel's Wired IP Settings

There are only two available methods of communicating to a target Master over the Internet: Wireless (via an internal card) or Wired (direct Ethernet connection). If you are not using an internal wireless card, you can only configure the connection parameters through the System Settings page. This type of communication can be established either via either a Dynamic IP Address (*DHCP*) or via a pre-reserved Static IP Address (*typically provided by your System Administrator*).

IP Settings section - Configuring a DHCP Address over Ethernet

1. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page.
2. Locate the IP Settings section of this page.

Even though the Host, Gateway, Primary DNS, Secondary DNS, and Domain fields appear on the two separate System Settings and Wireless Settings pages; ***the information populating these fields is identical.***
If the information within one of these fields is altered, the change is reflected on both pages within the altered field.
Example*: Domain is altered on Wireless Settings page, the value is then also changed within the Domain field of the System Settings page.*

3. Toggle the *DHCP/Static* field (***from the IP Settings section***) until the choice cycles to **DHCP**.

DHCP will register the unique MAC Address (factory assigned) on the panel and once the communication setup process is complete, reserve an IP Address, Subnet Mask, and Gateway values from the DHCP Server.

4. Press the optional *Host Name* field to open a Keyboard and enter the Host Name information.
5. Press **Done** after you are finished assigning the alpha-numeric string of the host name.
6. Do not alter any of the remaining greyed-out fields in the IP Settings section. *Once the panel is rebooted, these values are obtained by the unit and displayed in the DNS fields after power-up.*

This information can be found in either the: Workspace- System name > Define Device section of your code (that defines the properties for your panel), or in the Device Addressing/Network Addresses in the Tools > NetLinx Diagnostics dialog.

7. Press the **Back** button to return to the Protected Setup page.
8. Press the on-screen **Reboot** button to both save any changes and restart the panel.

IP Settings section - Configuring a Static IP Address over Ethernet

1. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page.
2. Locate the IP Settings section of this page.

Check with your System Administrator for a pre-reserved Static IP Address assigned to the panel. This address must be obtained before Static assignment of the panel continues.

3. Toggle the *DHCP/Static* field (***from the IP Settings section***) until the choice cycles to **Static**.
4. Press the *IP Address* field to open a Keyboard and enter the Static IP Address (*provided by your System Administrator*).
5. Press **Done** after you are finished entering the IP information.
6. Repeat the same process for the *Subnet Mask* and *Gateway* fields.
7. Press the optional *Host Name* field to open the Keyboard and enter the Host Name information.
8. Press **Done** after you are finished assigning the alpha-numeric string of the host name.

9. Press the Primary DNS field to open a Keyboard, enter the Primary DNS Address (provided by your System Administrator) and press **Done** when compete. Repeat this process for the Secondary DNS field.
10. Press the *Domain* field to open a Keyboard, enter the resolvable domain Address (*this is provided by your System Administrator and equates to a unique Internet name for the panel*), and press **Done** when complete.
11. Navigate to the Master Connection section of this page to begin configuring the communication parameters for the target Master.

Step 2: Choose a Master Connection Mode Setting

There are three Ethernet MODE settings used in the Master Connection section of the System Settings page. **URL is the most common method.**

- **Master Connection MODE** options:

- **URL** (**Uniform Resource Locator**) is the address that defines the route to a file on the Web or any other Internet facility.
  In this system, the panel acts as a "Client" and the Master acts as a Server (in that Clients attach to it).
- **LISTEN** sets the Modero panel to "listen" for broadcasts from the Master (using the panel IP from its URL list). In this system, the panel acts as a "Server" (in that Clients attach to it) and the Master acts as a "Client".
- **AUTO** is used to instruct the Modero to search for a Master that uses the same System Number (assigned within the Master Connection section) and resides on the same Subnet as itself. In this case, the Master has its UDP feature enabled.
  This **UDP** (**User Datagram Protocol**) is a protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
  This UDP enabling is done through a Telnet session on the Master. Refer to the particular NetLinx Master manual for more detailed information.

Step 3: Configure an Ethernet Connection Type

When using Ethernet as your communication method, the NetLinx Master must first be setup with either a Static IP or DHCP Address obtained from either NetLinx Studio or your System Administrator.

Before beginning:

1. Verify the panel has been configured to communicate either through an Ethernet cable (from the panel to a valid Ethernet Hub) or to a wirelessly (from the panel to a compatible Wireless Access Point (WAP)).

Before commencing, verify you are using the latest NetLinx Master firmware.

2. Verify that the NetLinx Master is receiving power and is communicating via an Ethernet connection with the PC running NetLinx Studio.
3. Connect the terminal end of the 12 VDC-compliant power supply cable to the power connector on the rear/side of the touch panel.
4. Verify the green Ethernet LED (from the rear Ethernet port on the Master) is illuminated (indicating a proper connection).

5. Verify the yellow LED (from the rear Ethernet port on the Master) is blinking (indicating communication).
6. After the panel powers-up, press and hold the grey Front Setup Access button (**for 3 seconds**) to proceed to the Setup page.
7. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page (FIG. 70).

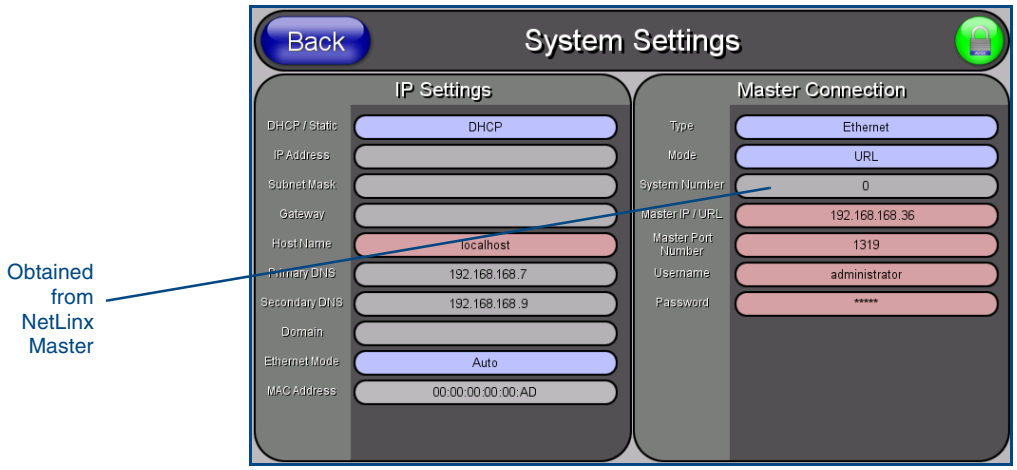


FIG. 70 System Settings page

Master Connection section - Virtual Master communication over Ethernet

NOTE

When configuring your panel to communicate with a Virtual Master (on your PC) via Ethernet, the Master IP/URL field must be configured to match the IP Address of the PC and make sure to use the Virtual System value assigned to the Virtual Master within NetLinx Studio.

Before beginning:

1. Verify the panel has been configured to communicate either through an Ethernet cable (connected from either the panel to a valid Ethernet Hub) or wireless to the Wireless Access Point.
2. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
3. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 71).
4. Click the **Communications Settings** button to open the Communications Settings dialog.
5. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.
6. Click on the **Virtual Master** radio box (*from the Transport Connection Option section*) to indicate you are wanting to configure the PC to communicate with a panel. Everything else such as the Authentication is greyed-out because you are not going through the Master's UI.
7. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the Virtual NetLinx Master Settings dialog (FIG. 71).

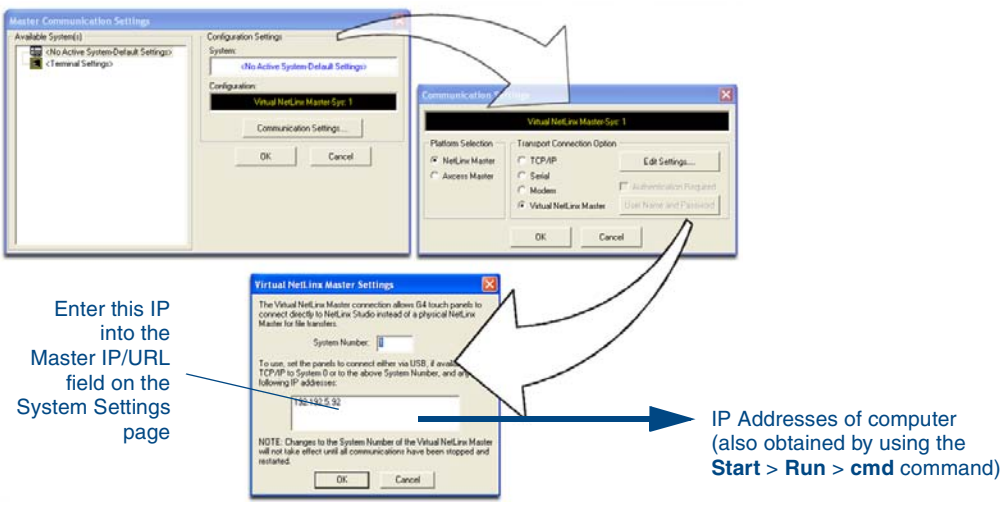

Enter this IP into the Master IP/URL field on the System Settings page
IP Addresses of computer (also obtained by using the Start > Run > cmd command)

FIG. 71 Assigning Communication Settings and TCP/IP Settings for a Virtual Master

8. From within this dialog enter the System number (***default is 1***) and note the IP Address of the target PC being used as the Virtual Master. This IP Address can also be obtained by following these procedures:
   - On your PC, click **Start > Run** to open the Run dialog.
   - Enter **cmd** into the Open field and click **OK** to open the command DOS prompt.
   - From the **C:\>** command line, enter **ipconfig** to display the IP Address of the PC. This information is entered into the *Master IP/URL* field on the panel.
9. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
10. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is one*.
11. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list.
12. Power-up your panel and press and hold the grey Front Setup Access button (**for 3 seconds**) to continue with the setup process and proceed to the Setup page.
13. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page (FIG. 72).

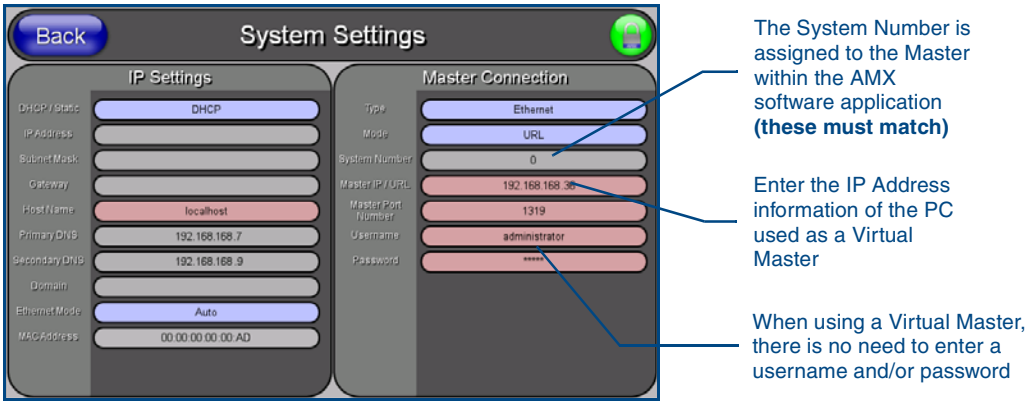


FIG. 72 Sample System Settings page (for Virtual Master communication)

14. Press the blue *Type* field (***from the Master Connection section***) until the choice cycles to the word **Ethernet.**
15. Press the *Mode* field until the choice cycles to the word **URL**.
    - By selecting **URL**, the System Number field becomes read-only (grey) because the panel pulls this value directly from the communicating target Master (virtual or not). A Virtual Master system value can be set within the active AMX software applications such as: NetLinx Studio, TPD4, or IREdit.
16. Press the *Master IP/URL* field to open a Keyboard and enter the IP Address of the PC used as the Virtual Master.
17. Click **Done** to accept the new value and return to the System Settings page.
18. Do not alter the Master Port Number value (*this is the default value used by NetLinx*).
19. Press the **Back** button to open the Protected Setup page.
20. Press the on-screen **Reboot** button to both save any changes and restart the panel.

Master Connection section - NetLinx Master Ethernet IP Address - URL Mode

In this mode, enter the System Number (**zero** for an unknown System Number) and the IP/URL of the Master (Master Port Number is defaulted to **1319**).

1. Press the blue *Type* field (***from the Master Connection section***) until the choice cycles to the word **Ethernet** (FIG. 72). Refer to the *System Settings Page* section on page 132 for more information about the fields on this page.
2. Press the *Mode* field until the choice cycles to the word **URL**.
    - By selecting **URL**, the System Number field becomes read-only (grey) because the panel pulls this value directly from the communicating target Master (virtual or not). A Virtual Master system value can be set within the active AMX software applications such as: NetLinx Studio, TPD4, or IREdit.

If the panel does not appear within the OnLine Tree tab of the Workspace window of NetLinx Studio, check to make sure that the NetLinx Master System Number (from within the Device Addressing dialog) is correctly assigned.

3. Press the *Master IP/URL* field to open a Keyboard and enter the Master IP Address **(obtained from the Diagnostics - Networking Address dialog of the NetLinx Studio application)**.
4. Click **Done** to accept the new value and return to the System Settings page.
5. Do not alter the Master Port Number value (*this is the default value used by NetLinx*).
6. Enter a username and password (*into their respective fields*) if the target Master has been previously secured.
7. Press the **Back** button to open the Protected Setup page.
8. Press the on-screen **Reboot** button to both save any changes and restart the panel.

Master Connection section - NetLinx Master Ethernet IP Address - Listen Mode

In this mode, you must add the Modero panel IP Address into the URL List of the Master (using NetLinx Studio). This mode sets the Modero panel to "listen" for broadcasts from the Master (using the panel IP from its URL list).

1. Obtain either a Static IP for the Modero panel (from your System Administrator) or a DHCP Address from the IP Settings of the System Settings page.
   - The *DHCP/Static* field (in the IP Settings section of the System Settings page) must be set to **DHCP** to get Dynamic IP information for the panel.
   - Press the on-screen **Reboot** (from the Protected Setup page) to both save any changes and restart the panel.
   - After power-up, press the grey Front Setup Access button for **3 seconds** to access the Setup page.
   - Navigate to the **Setup > Protected Setup > System Settings** page and note the newly obtained Dynamic IP Address information from the IP Settings section. This information is then entered into the URL List for the connected NetLinx Master.
2. Toggle the *Type* field until **Ethernet** is selected (*from the Master Connection section of the System Settings page*).
3. Press the *Mode* field (to set the connection Mode) until the choice cycles to the word **Listen**. *The System Number and Master IP/URL fields are then greyed-out.*
4. Enter a username and password (*into their respective fields*) if the target Master has been previously secured.
5. Select the **OnLine Tree** tab from the Workspace window.
6. Select **Diagnostics > URL Listing** from the Main menu (FIG. 73).

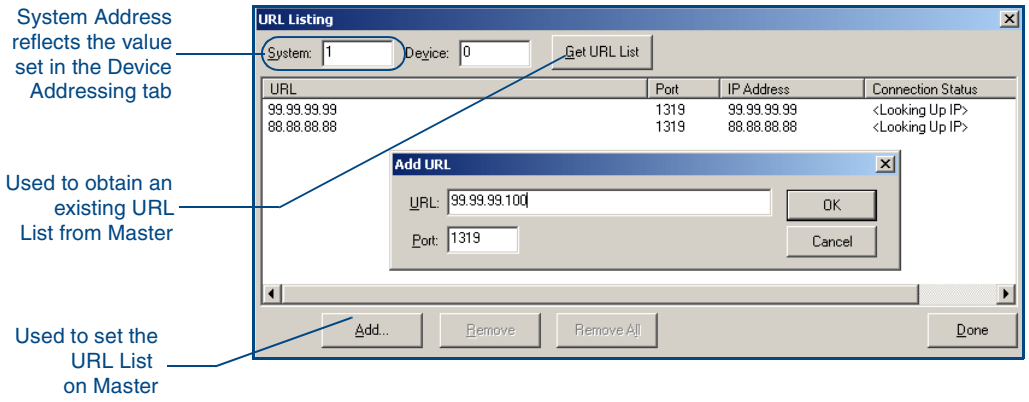


FIG. 73 URL List dialog

7. Enter the **System** and **Device** number for the specific Master associated with your panel (*as seen in the OnLine Tree tab*).
8. Click **Add** and enter the IP Address of the Modero touch panel into the *Add URL* dialog.
9. Click **OK** to enter your IP Address and add it to the list.
10. Click **Done** once you are finished adding your panel information to the list.
11. Press the on-screen **Reboot** button to save any changes and restart the panel.

Master Connection section - NetLinx Master Ethernet IP Address - Auto Mode

In this mode, enter the System Number of the NetLinx Master. This mode instructs the Modero to search for a Master that uses the same System Number (assigned within the Master Connection section) and **resides on the same Subnet as itself.**

1. Toggle the blue *Type* field until **Ethernet** is selected (*from the Master Connection section of the System Settings page*).
2. Press the *Mode* field until the choice cycles to the word **Auto**.
3. Press the *System Number* field to launch a Keypad and enter the value for the system number of the NetLinx Master. *This value can be obtained from the NetLinx Studio program > OnLine Tree of the Workspace window.*
4. Do not alter the IP Settings section, of the System Settings page, as these fields are not applicable to this connection mode.
5. Enter a username and password (*into their respective fields*) if the target Master has been previously secured.
6. Press the on-screen **Reboot** button to both save any changes and restart the panel.
7. Press the grey Front Setup Access button for **3 seconds** to open the Setup page and confirm there is an active connection.

The NetLinx Master and the Modero panel must both be on the same Subnet.

Using G4 Web Control® to Interact with a G4 Panel

The G4 Web Control feature allows you to use a PC to interact with a G4 enabled panel via the web. This feature works in tandem with the new browser-capable NetLinx Security firmware update (***build 300 or higher***). G4 Web Control is only available with the latest Modero panel firmware.

Refer to the *G4 Web Control Page* section on page 103 for more detailed field information.

*Verify your NetLinx Master (ME260/64 or NI-Series) has been installed with the latest firmware KIT file from **www.amx.com**. Refer to your NetLinx Master instruction manual for more detailed information on the use of the new web-based NetLinx Security.*

1. Press the grey Front Setup Access button for **3 seconds** to open the Setup page.
2. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
3. Enter ***1988*** into the Keypad's password field (***1988*** *is the default password*).

Clearing Password #5, from the initial Password Setup page, removes the need for you to enter the default password before accessing the Protected Setup page.

4. Press **Done** when finished.
5. Press the **G4 WebControl** button to open the G4 Web Control page (FIG. 74).
6. Press the **Enable/Enabled** button until it toggles to **Enabled** (*light blue color*).

FIG. 74 G4 Web Control page

7. The *Network Interface Select* field is read-only and displays the method of communication to the web. **Verify you have selected the proper interface connection as this field does not auto-detect the connection type being used (*see below*)**.
   - **Wired** is used when a direct Ethernet connection is being used for communication to the web. *This is the default setting if either no wireless interface card is detected or if both an Ethernet and wireless card connection is detected by the panel.*
   - **Wireless** is used when a wireless card is detected within the internal card slot. This method provides an indirect communication to the web via a pre-configured Wireless Access Point.
8. Press the *Web Control Name* field to open the Web Name keyboard.
9. From the Web Name keyboard, enter a unique alpha-numeric string to identify this panel. This information is used by the NetLinx Security Web Server to display on-screen links to the panel. *The on-screen links use the IP Address of the panel and not the name for communication* (FIG. 75).

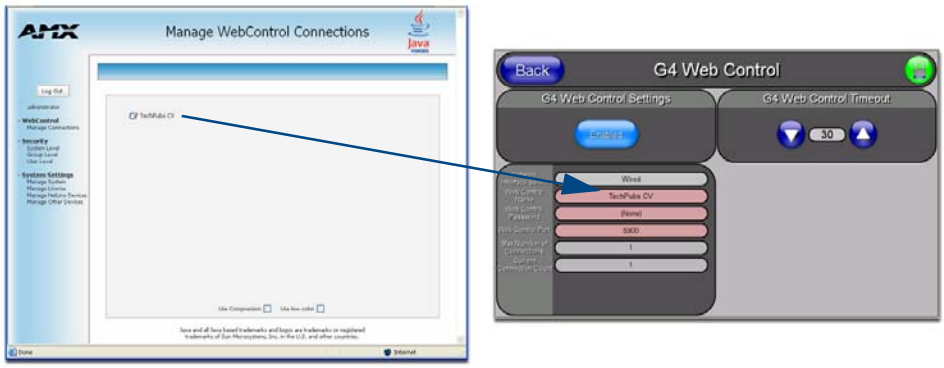


FIG. 75 Sample relationship between G4 Web Control and Mange WebControl Connections window

10. Press **Done** after you are finished assigning the alpha-numeric string for the Web Control name.
11. Press the *Web Control Password* field to open the Web Password keyboard.
12. From the Web Password keyboard, enter a unique alpha-numeric string to be assigned as the G4 Authentication session password associated with VNC web access of this panel.
13. Press **Done** after you are finished assigning the alpha-numeric string for the Web Control password.
14. Press the *Web Control Port* field to open the Web Port Number keypad.
15. Within the keypad, enter a unique numeric value to be assigned to the port the VNC Web Server is running on. The default value is ***5900***.

16. Press **Done** when you are finished entering the value. *The remaining fields within the G4 Web Control Settings section of this page are read-only and cannot be altered.*
17. Press the **Up/Down** arrows on either sides of the G4 Web Control *Timeout* field to increase or decrease the amount of time the panel can remain idle (***no cursor movements***) before the session is closed and the user is disconnected.
18. Press the **Back** button to open the Protected Setup page.
19. Press the on-screen **Reboot** button to save any changes and restart the panel.

NOTE

Verify your NetLinx Master's IP Address and System Number have been properly entered into the Master Connection section of the System Settings page.

Using your NetLinx Master to control the G4 panel

Refer to your particular NetLinx Master's instruction manual for detailed information on how to download the latest firmware from **www.amx.com**. This firmware build enables SSL certificate identification and encryption, HTTPS communication, ICSP data encryption, and disables the ability to alter the Master security properties via a TELNET session.

NOTE

In order to fully utilize the SSL encryption, your web browser should incorporate the an encryption feature. This encryption level is displayed as a Cipher strength.

Once the Master's IP Address has been set through NetLinx Studio version 2.x or higher:

1. Launch your web browser.
2. Enter the IP Address of the target Master (***ex: http://198.198.99.99***) into the web browser's *Address* field.
3. Press the **Enter** key on your keyboard to begin the communication process between the target Master and your computer.
   - Initially, the Master Security option is disabled (from within the **System Security** page) and no username and password is required for access or configuration.
   - Both HTTP and HTTPS Ports are enabled by default (via the **Manage System > Server** page).
   - If the Master has been previously configured for secured communication, click **OK** to accept the AMX SSL certificate (*if SSL is enabled*) and then enter a valid username and password into the fields within the *Login* dialog.
4. Click **OK** to enter the information and proceed to the Master's Manage WebControl Connections window.
5. This Manage WebControl Connections page (FIG. 76) is accessed by clicking on the **Manage connections** link (*within the Web Control section within the Navigation frame*). Once activated, this page displays links to G4 panels running the latest G4 Web Control feature (*previously setup and activated on the panel*).
6. Click on the G4 panel name link associated with the target panel. A secondary web browser window appears on the screen (FIG. 77).
7. Click **Yes** from the Security Alert popup window to agree to the installation of the G4 WebControl application on your computer. This application contains the necessary Active X and VNC client applications necessary to properly view and control the panel pages from your computer.

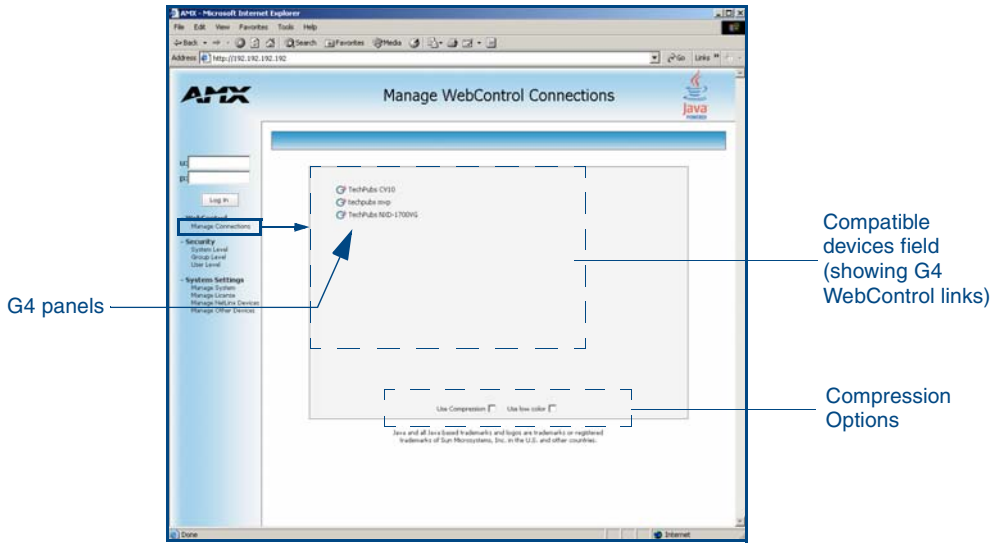


FIG. 76 Manage WebControl Connections page (populated with compatible panels)

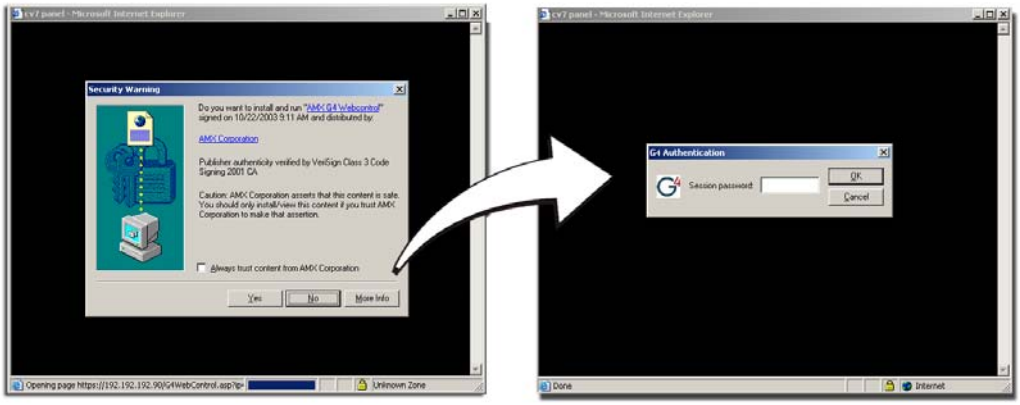


FIG. 77 Web Control VNC installation and Password entry screens

NOTE

The G4 Web Control application is sent by the panel to the computer that is used for communication. Once the application is installed, this popup will no longer appear. This popup will only appear if you are connecting to the target panel using a different computer.

8. In some cases, you might get a *Connection Details* dialog (FIG. 78)requesting a VNC Server IP Address. This is the IP Address not the IP of the Master but of the target touch panel. Depending on which method of communication you are using, it can be found in either the:
   - **Wired Ethernet** - System Settings > IP Settings section within the *IP Address* field.
   - **Wireless** - Wireless Settings > IP Settings section within the *IP Address* field.
   - If you do not get this field continue to step 9.
9. If a WebControl password was setup on the G4 WebControl page, a G4 Authentication Session password dialog box appears on the screen within the secondary browser window.
10. Enter the Web Control session password into the *Session Password* field (FIG. 77). *This password was previously entered into the Web Control Password field within the G4 Web Control page on the panel.*

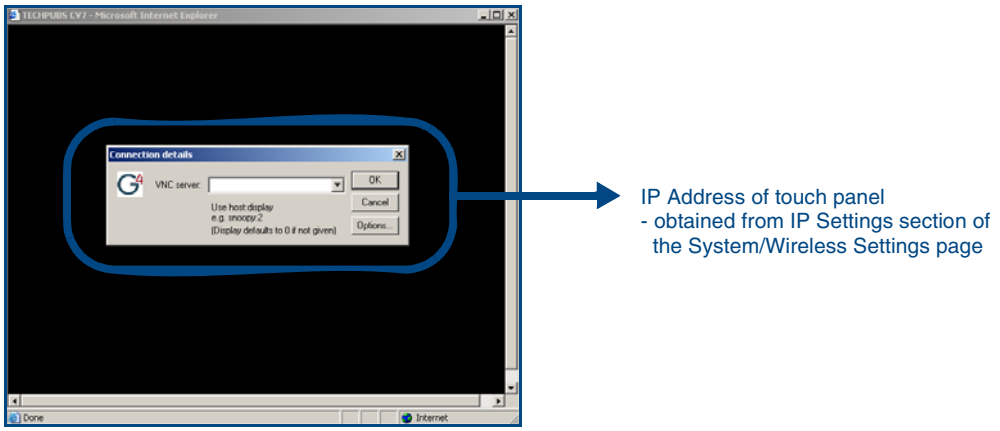


FIG. 78 Connection Details dialog

11. Click **OK** to send the password to the panel and begin the session. A confirmation message appears stating *"Please wait, Initial screen loading."*.

The secondary window then becomes populated with the same G4 page being displayed on the target G4 panel. A small circle appears within the on-screen G4 panel page and corresponds to the location of the mouse cursor. A left-mouse click on the computer-displayed panel page equates to an actual touch on the target G4 panel page.

Upgrading Modero Firmware

Before beginning the Upgrade process:

- Setup and configure your NetLinx Master. Refer to the your particular NetLinx Master Instruction Manual for detailed setup procedures.
- Calibrate and prepare the communication pages on the Modero panel for use. Refer to the *Panel Calibration* section on page 49.

NOTE

The latest CV10 firmware kit file is now panel-specific.
Only CV10 firmware should be loaded onto this specific panel type.
This new firmware also provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.

- Refer to the NetLinx Studio version 2.x Help file for more information on uploading files via Ethernet.
- Configure your panel for either direct connect or wireless communication. Refer to the *Configuring Communication* section on page 51 for more information.

WARNING

It is recommended that firmware Kit files only be transferred over a direct Ethernet connection and only when the panel is connected to a power supply.
If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.

The process of updating firmware involves the use of a communicating NetLinx Master. The required steps for updating firmware to a Modero panel are virtually identical to those necessary for updating Kit files to a NetLinx Master (*except the target device is a panel instead of a Master*). Refer to either your Master's literature or Studio 2.x Help file for those procedures.

WARNING

A touch panel which is not using a valid username and password will not be able to communicate with a secured Master. If you are updating the firmware on or through a panel which is not using a username or password field, you must first remove the Master Security feature to establish an unsecured connection.

Upgrading the Modero Firmware via the USB port

Before beginning with this section, verify your panel is both powered and the Type-A USB connector is securely inserted into the PC's USB port. **The panel must be powered-on before connecting the mini-USB connector to the panel.**

WARNING

Establishing a USB connection between the PC and the panel, prior to installing the latest NetLinx Studio and TPDesign4 applications will cause a failure in the USB driver installation.
This driver must first be saved to the PC as part of the new NetLinx Studio and TPDesign4 application installations.

Step 1: Configure the panel for a USB Connection Type

1. After the installation of the USB driver has been completed; confirm the proper installation of the large Type-A USB connector to the PC's USB port, and restart your machine.
2. After the CV7 panel powers-up, press and hold the grey Front Setup Access button (**for 3 seconds**) to continue with the setup process and proceed to the Setup page.
3. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page.

4. Toggle the blue *Type* field (***from the Master Connection section***) until the choice cycles to **USB**.

NOTE

***ALL** fields are then greyed-out and read-only, but still display any previous network information.*

5. Press the **Back** button on the touch panel to return to the Protected Setup page.
6. Press the on-screen **Reboot** button to both save any changes and **restart the panel.** *Remember that the panel's connection type must be set to **USB** prior to rebooting the panel and prior to inserting the USB connector.*
7. **ONLY AFTER** the unit displays the first panel page, **THEN** insert the mini-USB connector into the Program Port on the panel. It may take a minute for the panel to detect the new connection and send a signal to the PC (*indicated by a green System Connection icon*).
   - If a few minutes have gone by and the System Connection icon still does not turn green, complete the procedures in the following section to setup the Virtual Master and refresh the System from the Online Tree. This action sends out a request to the panel to respond and completes the communication (turning the System Connection icon green).
8. Navigate back to the System Connection page.

Step 2: Prepare NetLinx Studio for communication via the USB port

1. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
2. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 79).

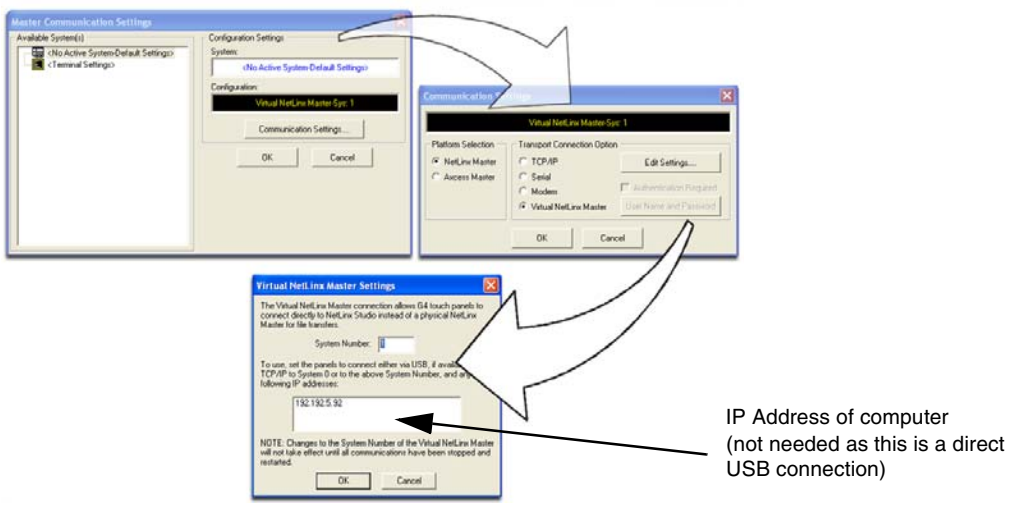


FIG. 79 Assigning Communication Settings for a Virtual Master

3. Click the **Communications Settings** button to open the *Communications Settings* dialog.
4. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.
5. Click on the **Virtual Master** radio box (*from the Transport Connection Option section*) to indicate you are wanting to configure the PC to communicate directly with a panel. Everything else such as the Authentication is greyed-out because you are not going through the Master's UI.

6. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the *Virtual NetLinx Master Settings* dialog (FIG. 79).
7. From within this dialog enter the System number (default is **1**).
8. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
9. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is one*.
10. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list.
    The panel will not appear as a device below the virtual system number (in the Online Tree tab) until both the system number used in step 7 for the Virtual NetLinx Master (VNM) is entered into the Master Connection section of the System Connection page and the panel is restarted.

NOTE

If the G4 panel does not appear, refer to the Troubleshooting section on page 185 *for more information.*

Step 3: Confirm and Upgrade the firmware via the USB port

Use the CC-USB Type-A to Mini-B 5-wire programming cable (**FG10-5965**) to provide communication between the mini-USB Program port on the touch panel and the PC. This method of communication is used to transfer firmware Kit files and TPD4 touch panel files.

NOTE

A mini-USB connection is only detected after it is installed onto an active panel. Connection to a previously powered panel which then reboots, allows the PC to detect the panel and assign an appropriate USB driver.

1. Verify this direct USB connection (Type-A on the panel to mini-USB on the panel) is configured properly using the steps outlined in the previous two sections.
2. With the panel already configured for USB communication and the Virtual Master setup within NetLinx Studio, its now time to verify the panel is ready to receive files.
3. After the Communication Verification dialog window verifies active communication between the Virtual Master and the panel, click the **OnLine Tree** tab in the Workspace window (FIG. 80) to view the devices on the Virtual System. *The default System value is one*.
4. Right-click on the System entry (FIG. 80) and select **Refresh System** to re-populate the list. Verify the panel appears in the **OnLine Tree** tab of the Workspace window.
   The default Modero panel value is 10001.

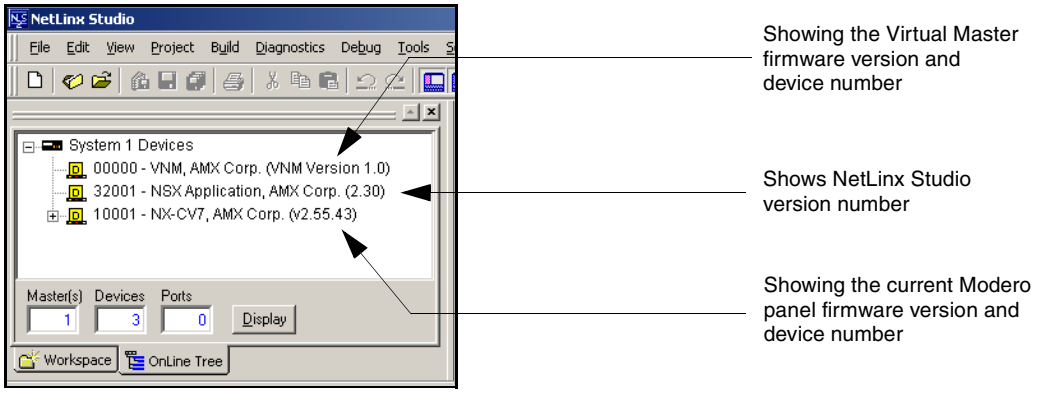

NetLinx Studio
File Edit View Project Build Diagnostics Debug Tools
System 1 Devices
00000 - VNM, AMX Corp. (VNM Version 1.0)
32001 - NSX Application, AMX Corp. (2.30)
10001 - NX-CV7, AMX Corp. (v2.55.43)
Master(s) Devices Ports
1 3 0
Display
Workspace
OnLine Tree
Showing the Virtual Master firmware version and device number
Shows NetLinx Studio version number
Showing the current Modero panel firmware version and device number

FIG. 80 NetLinx Workspace window (showing the panel connection via a Virtual NetLinx Master)

NOTE

The latest CV10 firmware kit file is now panel-specific.
Only CV10 firmware should be loaded onto this specific panel type.
This new firmware also provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.

5. If the panel firmware being used is not current, download the latest Kit file by first logging in to **www.amx.com** and then navigate to **Tech Center > Firmware Files** and from within the **Modero** section of the web page locate your Modero panel.
6. Click on the desired Kit file link and after you've accepted the Licensing Agreement, verify you have downloaded the Modero Kit file to a known location.
7. From within Studio, select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (**B** in FIG. 81). Verify the panel's System and Device number values (**B** in FIG. 81) match those values listed within the System folder in the **OnLine Tree** tab of the Workspace window (**A** in FIG. 81).

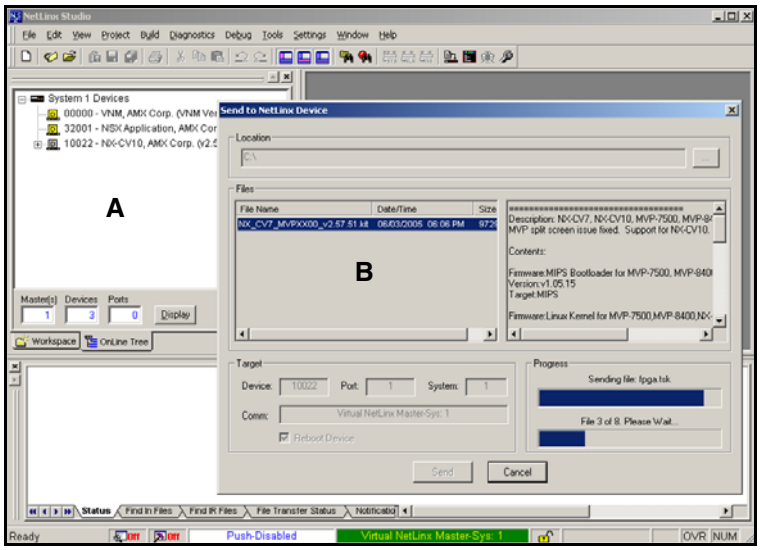


FIG. 81 Using USB for a Virtual Master transfer

8. Select the panel's Kit file from the **Files** section.
9. Enter the **Device** value associated with the panel and the **System** number associated with the Master (*listed in the OnLine Tree tab of the Workspace window*). *The Port field is greyed-out.*
10. Click the **Reboot Device** checkbox. This causes the touch panel to reboot after the firmware update process is complete. *The reboot of the panel can take up 30 seconds after the firmware process has finished.*
11. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog (**B** in FIG. 81).
12. As the panel is rebooting, temporarily unplug the USB connector on the panel until the panel has completely restarted.
13. Once the first panel page has been displayed, reconnect the USB connector to the panel.
14. Right-click the associated System number and select **Refresh System**. This causes a refresh of all project systems, establishes a new connection to the Master, and populates the System list with devices on your particular system.
15. Confirm the panel has been properly updated to the correct firmware version.

Upgrading the Modero Firmware via Ethernet (IP Address)

Before beginning with this section, verify that your panel is powered and connected to the NetLinx Master through an Ethernet connection (direct or wireless).

Step 1: Prepare the Master for communication via an IP

1. Obtain the IP Address of the NetLinx Master from your System Administrator. If you do not have an IP Address for the Master, refer to your particular Master's instruction manual for more information on obtaining this IP Address using NetLinx Studio 2.x.
   - From the **Online Tree** tab of the Workspace window, select the NetLinx Master.
   - Follow steps outlined in either the *Obtaining or Assigning the Master's IP Address* sections from your particular NetLinx Master instruction manual to use an address.
   - Note the IP Address and Gateway information.
2. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
3. Select **Settings > Master Communication Settings** from the Main menu to open the Master Communication Settings dialog (FIG. 82).

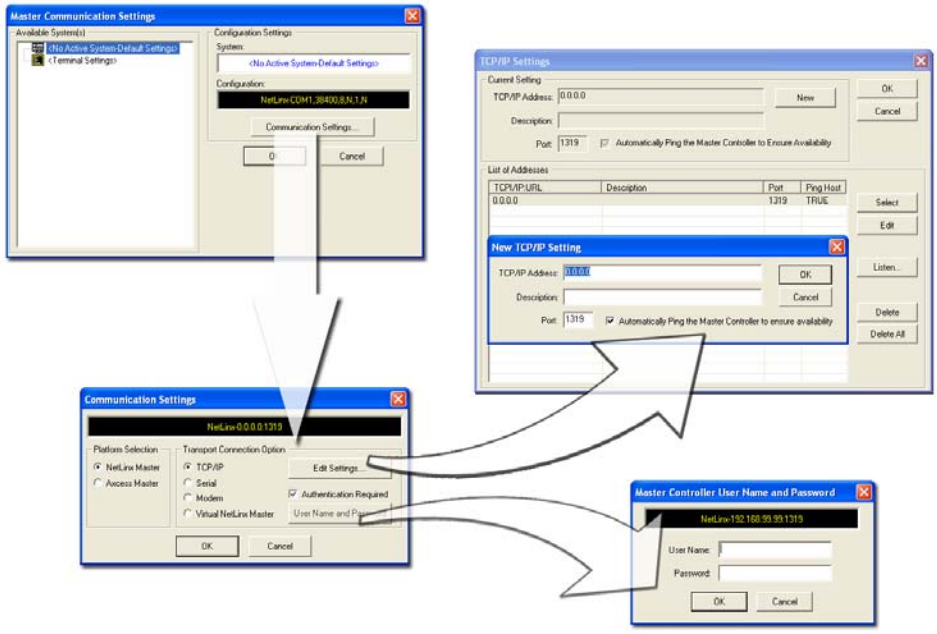


FIG. 82 Assigning Communication Settings and TCP/IP Settings

4. Click the **Communications Settings** button to open the Communications Settings dialog.
5. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate you are working with a NetLinx Master (such as the NXC-ME260/64 or NI-Series of Integrated Controllers).
6. Click on the **TCP/IP** radio button (*from the Transport Connection Option section*) to indicate you are connecting to the Master through an IP Address.
7. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the TCP/IP Settings dialog (FIG. 82). This dialog contains a series of previously entered IP Address/URLs and their associated names, all of which are stored within Studio and are user-editable.

8. Click the **New** button to open the New TCP/IP Settings dialog where you can enter both a previously obtained DHCP or Static IP Address and an associated description for the connection into their respective fields.
9. Place a checkmark within the *Automatically Ping the Master Controller to ensure availability* radio box to make sure the Master is initially responding online before establishing full communication.
10. Click **OK** to close the current New TCP/IP Settings dialog and return to the previous TCP/IP Settings dialog where you must locate your new entry within the List of Addresses section.
11. Click the **Select** button to make that the currently used IP Address communication parameter.
12. Click **OK** to return to the Communications Settings dialog and place a checkmark within the *Authentication Required* radio box if your Master has been previously secured with a username/password.
13. Click on the **Authentication Required** radio box (if the Master is secured) and then press the **User Name and Password** button to open the Master Controller User Name and Password dialog.
14. Within this dialog, you must enter a previously configured username and password (with sufficient rights) before being able to successfully connect to the Master.
15. Click **OK** to save your newly entered information and return to the previous Communication Settings dialog where you must click **OK** again to begin the communication process to your Master.

If you are currently connected to the assigned Master, a popup asks whether you would want to temporarily stop communication to the Master and apply the new settings.

16. Click **Yes** to interrupt the current communication from the Master and apply the new settings.
17. Click **Reboot** (*from the Tools > Reboot the Master Controller dialog*) and wait for the System Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
18. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.
19. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
20. Right-click the associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system. *The communication method is then highlighted in green on the bottom of the NetLinx Studio window.*

Step 2: Prepare the panel for communication via an IP

1. Press the blue *Type* field (*from the Master Connection section*) until the choice cycles to the word **Ethernet**.
2. Press the blue *Mode* field until the choice cycles to the word **URL**.
   - By selecting **URL**, the System Number field becomes read-only (grey) because the panel pulls this value directly from the communicating target Master (virtual or not). A Virtual Master system value can be set within the active AMX software applications such as: NetLinx Studio, TPD4, or IREdit.
3. Press the red *Master IP/URL* field to open a Keyboard and enter the NetLinx Master's IP Address (**obtained from the Diagnostics - Networking Address dialog of the NetLinx Studio application**).
4. Click **Done** to accept the new value and return to the System Configuration page.
5. Do not alter the Master Port Number value (*this is the default value used by NetLinx*).

6. Press the **Back** button to return to the Protected Setup page and press the on-screen **Reboot** button to restart the panel and save any changes.

Step 3: Verify and Upgrade the panel firmware via an IP

1. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one.*
2. Right-click the associated System number (from the Workspace window) and select **Refresh System** to detect of all devices on the current system, establish a new connection to the Master, and refresh the System list with devices on that system.
3. After the Communication Verification dialog window verifies active communication between the PC and the Master, verify the panel appears in the **OnLine Tree** tab of the Workspace window (FIG. 83). *The default Modero panel value is 10001.*

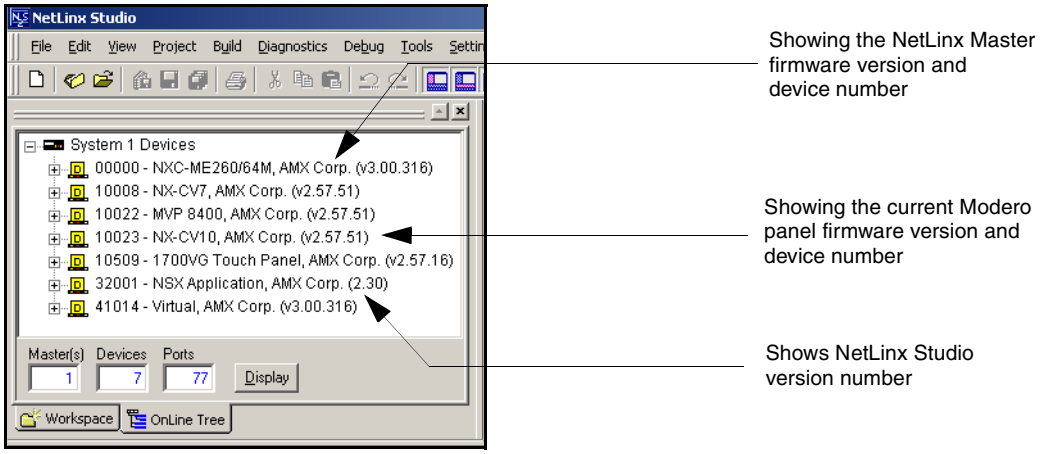

NetLinx Studio
File Edit View Project Build Diagnostics Debug Tools Settin
System 1 Devices
00000 - NXC-ME260/64M, AMX Corp. (v3.00.316)
10008 - NX-CV7, AMX Corp. (v2.57.51)
10022 - MVP 8400, AMX Corp. (v2.57.51)
10023 - NX-CV10, AMX Corp. (v2.57.51)
10509 - 1700VG Touch Panel, AMX Corp. (v2.57.16)
32001 - NSX Application, AMX Corp. (2.30)
41014 - Virtual, AMX Corp. (v3.00.316)
Master(s) Devices Ports
1 7 77
Display
Workspace
OnLine Tree
Showing the NetLinx Master firmware version and device number
Showing the current Modero panel firmware version and device number
Shows NetLinx Studio version number

FIG. 83 NetLinx Workspace window (showing connected Modero panel)

NOTE

The panel firmware is shown on the right of the listed panel.

4. If the panel firmware being used is not current, download the latest Kit file by first logging in to **www.amx.com** and then navigate to **Tech Center > Firmware Files** and from within the **Modero** section of the web page locate your Modero panel.

NOTE

The latest CV10 firmware kit file is now panel-specific.
Only CV10 firmware should be loaded onto this specific panel type.
This new firmware also provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.

5. Click on the desired Kit file link and after you've accepted the Licensing Agreement, verify you have downloaded the Modero Kit file to a known location.
6. From within Studio, select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (FIG. 84). Verify the panel's System and Device number values match those values listed within the System folder in the **OnLine Tree** tab of the Workspace window.
7. Select the panel's Kit file from the **Files** section (FIG. 84).
8. Enter the **Device** value associated with the panel and the **System** number associated with the Master (*listed in the OnLine Tree tab of the Workspace window*). *The Port field is greyed-out.*

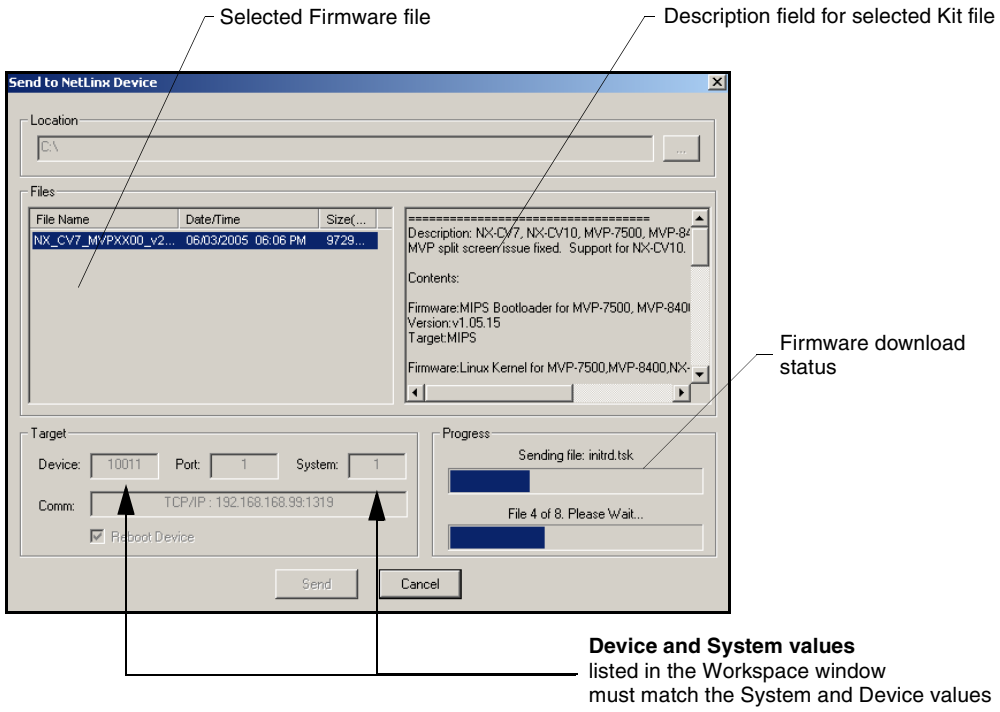


FIG. 84 Send to NetLinx Device dialog (showing Modero firmware update via IP)

9. Click the **Reboot Device** checkbox. This causes the touch panel to reboot after the firmware update process is complete. *The reboot of the panel can take up 30 seconds after the firmware process has finished.*
10. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog (FIG. 84).
11. Click **Close** (*after the panel reboots*) to return to the main program.
12. Right-click the associated System number and select **Refresh System**. This causes a refresh of all project systems, establishes a new connection to the Master, and populates the System list with devices on your particular system.
13. Confirm the panel has been properly updated to the correct firmware version.

Firmware Pages and Descriptions

This section describes each firmware page and their specific functional elements.

Setup Navigation Buttons

These Setup Navigation Buttons (FIG. 85) appear on the left of the panel screen when the Setup page is currently active.

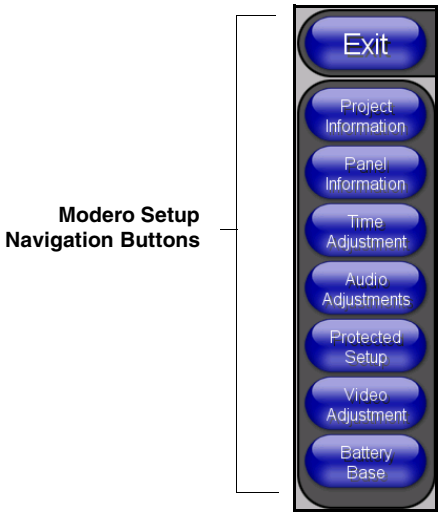


FIG. 85 Setup Navigation Buttons

These Navigation Buttons are specific to these Modero panels and include the specific elements described in the following table:

Setup Navigation Button Elements	
Project Information:	Press the Project Information button to access the Project Information and view the TPD4 project file properties currently loaded on the selected panel ***(read-only).*** • Refer to the *Project Information Page* section on page 92 for more detailed information.
Panel Information:	Press the Panel Information button to access the Panel Information page and view panel specific information such as resolution, memory, etc. ***(read-only).*** • Refer to the *Panel Information Page* section on page 93 for more detailed information.
Time Adjustment:	Press the Time Adjustment button to access the Time Adjustment page where you can alter the time and date settings on the Master. • Refer to the *Time & Date Setup Page* section on page 94 for more detailed information.
Audio Adjustments:	Press the Audio Adjustments button to access the Volume page where you can alter the audio parameters on the Modero panel. • Refer to the *Volume Page* section on page 96 for more detailed information.

Setup Navigation Button Elements (Cont.)	
Protected Setup:	Press the Protected Setup button to access the Protected Setup page section that provides access to the panel's sensors, calibration features, and connection settings. • Refer to both the *Protected Setup Navigation Buttons* section on page 100 and *Protected Setup Page* section on page 101 for more detailed information.
Video Adjustment:	Press the Video Adjustment button to access the Video Adjustment page where you can set the video properties for incoming video. • This button only appears on Color Video (CV) capable touch panels. • Refer to the *Video Adjustment Page* section on page 97 for more detailed information.
Battery Base:	Press the Battery Base button to access the Battery Base page where you can modify and monitor NXT-BP Modero Power Pack parameters. • This button only appears when a Modero Table Top panel (NXT) is connected to an NXA-BASE/B battery base. • Refer to the *Battery Base Page* section on page 98 for more detailed information.

Setup Page

This page (FIG. 86) centers around basic Modero panel properties such as: Connection Status of the panel, Display Timeout, Inactivity Page Flip Time, Inactivity page file, and the Panel Brightness.

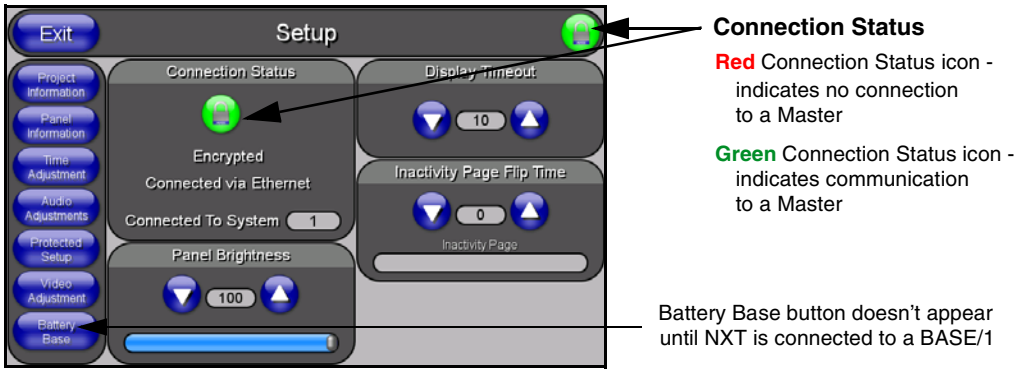


FIG. 86 Setup page

The elements of the Setup page are described in the table below:

Setup Page Elements	
Exit:	Returns you to the Main touch panel page. In this case, the previous page is the default Main page.
Connection Status icon:	This visual display of the connection status allows the user to have a current update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).

Setup Page Elements (Cont.)	
Connection Status:	Displays whether the panel is communicating externally, the encryption status of the communicating Master, what connection type is being used (*Ethernet or USB*), and what System the panel is a part of. This visual display of the connection status is also reflected at the upper-right of each firmware page. This allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • When a connection is established, the message displayed is either: "*Connected via Ethernet* " or "*Connected via USB* ". • If no connection can be established by the Modero panel, it will continue to try and establish a connection while displaying: "*Attempting via ...*". • The word "*Encrypted*" appears only when an encrypted connection is established with a target Master. • The panel must be rebooted before incorporating any panel communication changes and detecting any active Ethernet connections. ***The Ethernet connection is not detected until after a reboot.***
Display/Panel Timeout:	Sets the length of time the panel can remain idle before activating the sleep mode. When the device goes into sleep mode, the LCD is powered-down. • Press the UP/DN buttons to increase/decrease the time until the panel times out. Range = 0 - 240 minutes. • Use this button to set the timeout value to zero and disable the sleep mode. • Note: Display timeout values affect battery performance. Small timeout values increase the life of the battery charge. Greater timeout values may require more frequent battery charging.
Inactivity Page Flip Timeout:	Sets the number of minutes of inactivity before the panel automatically flips to a pre-selected touch panel page. When the device goes into this inactivity mode, the LCD does not power-down. • Press the UP/DN buttons to increase/decrease the time the panel can remain inactive before it flips to the preset page. Range = 0 - 240 minutes. • Use this button to set the timeout value to zero and disable the inactivity page flip mode. • The touch panel page used for the Inactivity page flip is shown within a small Inactivity Page field.
Panel Brightness:	Sets the display brightness level of the panel. • Press the UP/DN buttons to adjust the brightness level. Range = 0 - 100. • The on-screen bargraph can be dragged to adjust the Brightness level which is then reflected as a corresponding numeric value within the *Panel Brightness* field.

Project Information Page

The Project Information page displays the TPDesign4 (TPD4) project file properties currently loaded on the selected Modero panel (FIG. 87). Refer to the *TPDesign4 Touch Panel Program* instruction manual for more specific information on uploading TPDesign4 files to a panel.

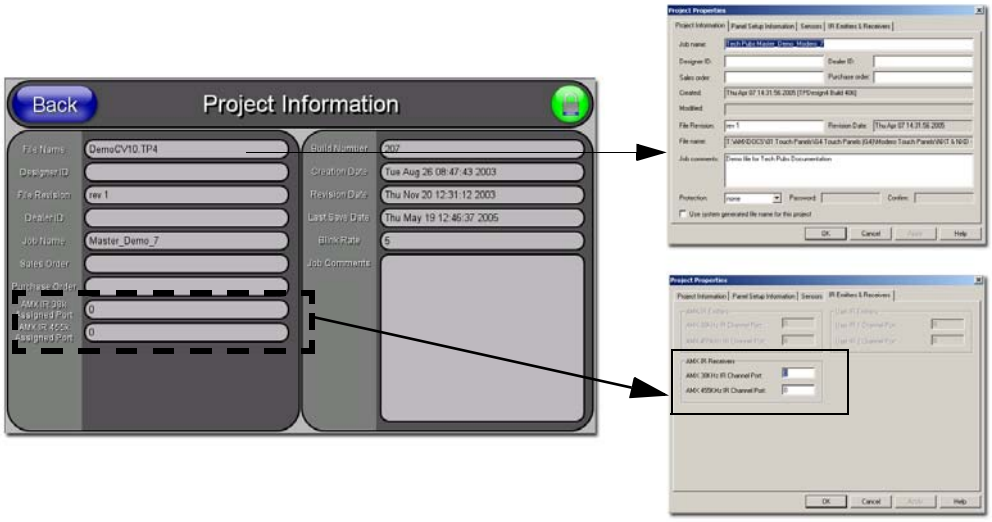


FIG. 87 Project Information page (showing the TPD4 project properties tabs)

The elements of the Project Information page are described in the table below:

Project Information Page Elements	
Back:	Returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
File Name:	Displays the name of the TPDesign4 project file downloaded to the panel.
Designer ID:	Displays the designer information.
File Revision:	Displays the revision number of the file.
Dealer ID:	Displays the dealer ID number (*unique to every dealer and entered in TPD4*).
Job Name:	Displays the job name.
Sales Order:	Displays the sales order information.
Purchase Order:	Displays the purchase order information.
AMX IR 38k Assigned Port:	Displays the AMX 38 kHz IR channel port used by the IR receiver on the panel. • This information is pulled by the panel from *AMX IR Receivers* section of the TPD4 Project Properties > IR Emitters & Receivers tab. • For IR reception, this is the port that reports a push on for the corresponding IR code. • IR receivers and transmitters on G4 panels share the device address number of the panel.

Project Information Page Elements (Cont.)	
AMX IR 455k Assigned Port:	Displays the AMX 455 kHz IR channel port used by the IR receiver on the panel. This information is pulled by the panel from *AMX IR Receivers* section of the TPD4 Project Properties > IR Emitters & Receivers tab. • For IR reception, this is the port that reports a push on for the corresponding IR code. • IR receivers and transmitters on G4 panels share the device address number of the panel.
Build Number:	Displays the build number information of the TPD4 software used to create the project file.
Creation Date:	Displays the project creation date.
Revision Date:	Displays the last revision date for the project.
Last Save Date:	Displays the last date the project was saved.
Blink Rate:	Displays the feedback blink rate (10th of second).
Job Comments:	Displays any comments associated to the job. These comments are taken from the TPD4 project file.

Panel Information Page

The Panel Information page (FIG. 88) centers around Modero panel properties such as: resolution used, on-board memory, firmware, address/channel information, and string information.

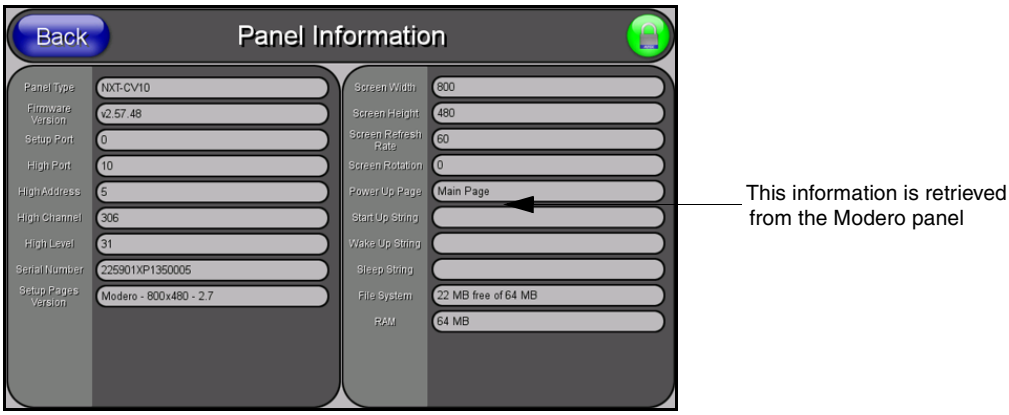


FIG. 88 Panel Information page (takes its' information from the touch panel)

The elements of the Panel Information page are described in the table below:

Panel Information Page Elements	
Back:	Returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Panel Type:	Displays the model of the Modero panel being used.
Firmware Version:	Displays the G4 firmware version being used by the panel. • Verify you have the latest version from **www.amx.com**.

Panel Information Page Elements (Cont.)	
Setup Port:	Displays the setup port information/value being used by the panel.
High Port:	Displays the high port (port count) value for the panel.
High Address:	Displays the high address (address count) value for the panel.
High Channel:	Displays the high channel (channel count) value for the panel.
High Level:	Displays the high level (level count) value being used by the panel.
Serial Number:	Displays the specific serial number value assigned to the panel.
Setup Pages Version:	Displays the type and version of the Setup pages being used by the panel.
Screen Width:	Displays the pixel width being used to display the incoming video signal on the Modero panel. • Maximum available screen width on a CV10 Modero panel is 800 pixels.
Screen Height:	Displays the pixel height being used to display the incoming video signal on the Modero panel. • Maximum available screen height on a CV10 Modero panel is 480 pixels.
Screen Refresh Rate:	Displays the video refresh rate applied to the incoming video signal from the panel. *Default rate is 60.*
Screen Rotation:	Displays the degree of rotation applied to the on-screen image.
Power Up Pages:	Displays the first touch panel page assigned for display after the device is powered-up. • This information is taken from the TPD4 project file. • Most projects begin with a Main page.
Start Up String:	Displays the start-up string.
Wake Up String:	Displays the wake up string used after an activation from a timeout.
Sleep String:	Displays the sleep string used during a panel's sleep mode.
File System:	Displays the amount of Compact Flash memory available on the Modero panel.
RAM:	Displays the available RAM (or Extended Memory module) on the Modero panel.

Time & Date Setup Page

The Time & Date Setup page (FIG. 89) allows you to alter/set the time and date information on the NetLinx Master. If either the Time/Date is modified on this page (*then updated to the Master by pressing the Set Time button*), all devices communicating to that target Master will then be updated to reflect the new information.

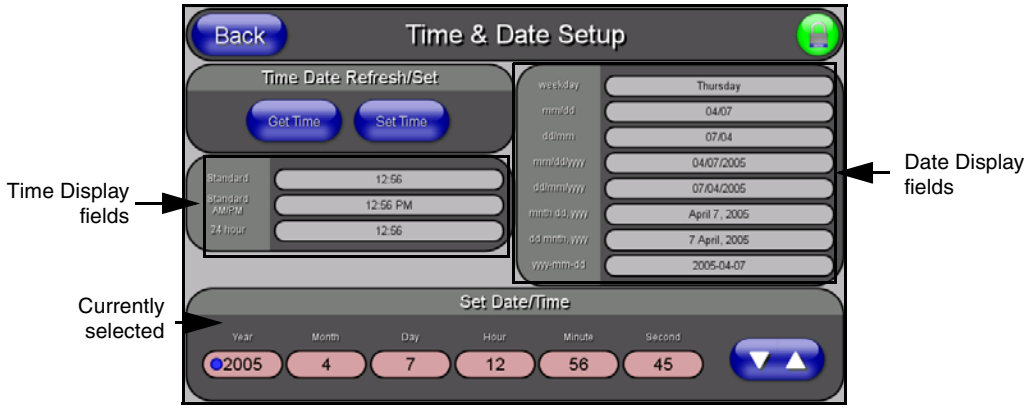


FIG. 89 Time and Date Setup page

The only way to modify a panel's time, without altering the Master, is to use NetLinx Code.

The elements of the Time & Date Setup page are described in the table below:

Time & Date Setup Page Elements	
Back:	Returns you to the previously active touch panel page without saving changes (*to save changes, use the Set Time button*).
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Time Date Refresh/Set:	This section provides you with two options: • The **Get Time/Date** button retrieves the Time and Date information from the Master. • The **Set Time/Date** button sets the Master to retain and save any time/date modifications made on the Time and Date Setup page.
Time Display fields:	• These fields display the time in three formats: STANDARD, STANDARD AM/PM, and 24 HOUR.
Date Display fields:	• These fields display the calendar date information in several different formats.
Set Date/Time:	This section provides a user with both UP/DN arrow buttons to alter the Master's calendar date and time. The blue circle indicates which field is currently selected. • Select the **Year** field and use the UP/DN buttons to alter the year value (range = 2000 - 2037). • Select the **Month** field and use the UP/DN buttons to alter the month value (range = 1 - 12). • Select the **Day** field and use the UP/DN buttons to alter the day value (range = 1 - 31). • Select the **Hour** field and use the UP/DN buttons to alter the hour value (24-hour military). • Select the **Minute** field and use the UP/DN buttons to alter the minute value (range = 0 - 59). • Select the **Second** field and use the UP/DN buttons to alter the second value (range = 0 - 59).

Modero touch panels do not have an on-board clock. This page both receives and sets the time/date of the NetLinx Master.

Volume Page

The Volume page (FIG. 90) (*accessed by pressing the Audio Adjustments button on the Setup page*) allows you to adjust the master volume parameters and default panel sounds on the panel.

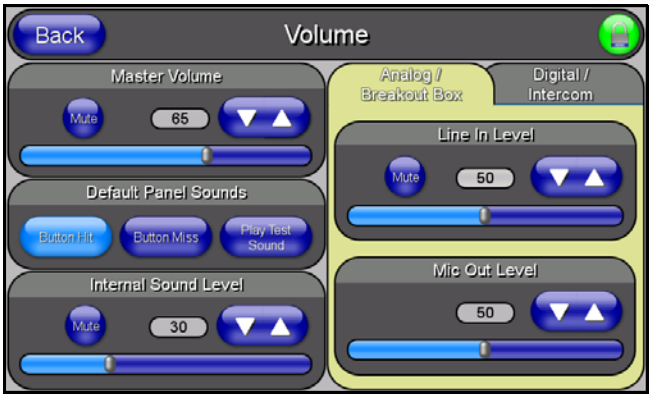


FIG. 90 Volume configuration page

The elements of the Volume page are described in the table below:

Volume Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Master Volume:	This section allows you to alter the current master volume level: • Use the UP/DN buttons to adjust the volume level (range = 0 - 100). • The Master Volume bargraph indicates the current volume level. • The **Mute** button toggles the Mute feature.
Default Panel Sounds:	Sets the Modero panel to play various sounds. • Activating the **Button Hit** button plays a default sound when you touch an active button. • Activating the **Button Miss** button plays a default sound when you touch a non-active button or any area outside of the active button • The **Play Test Sound** button plays a test WAV/MP3 file over the panel's internal speakers.
Internal Sound Level:	This section allows you to adjust the current sound level on the internal panel speaker: • Use the UP/DN buttons to adjust the volume output on the internal speakers (range = 0 - 100). • The Internal Sound Level bargraph indicates the current sound level. • The **Mute** button mutes the volume.

Volume Page Elements (Cont.)	
Analog/Breakout Box:	
Line In Level:	Allows you to adjust the current Line-In volume level (being received from the communicating breakout box). • Use the UP/DN buttons to adjust the Line-In volume level (range = 0 - 100). • The Line-In Level bargraph indicates the current Line-In level. • The **Mute** button mutes the Line-In volume.
Mic Out Level:	Allows you to adjust the current Microphone volume level (being received from the communicating breakout box). • Use the UP/DN buttons to adjust the Microphone volume level (range = 0 - 100). • The Mic Out Level bargraph indicates the current Mic Out level.

Supported sampling rates for WAV

The following is a listing of supported sampling rates associated for WAV files played on CV10 panels. Some WAV files currently played on Modero's may not work on these panels. The supported sampling rates for WAV files are:

Supported WAV Sampling Rates	
• 48000 Hz	• 16000 Hz
• 44100 Hz	• 12000 Hz
• 32000 Hz	• 11025 Hz
• 24000 Hz	• 8000 Hz
• 22050 Hz	

Protected Setup Page

This button opens the Protected Setup page which centers around the properties used by the panel to properly communicate with the NetLinx Master. Refer to both the *Protected Setup Navigation Buttons* section on page 100 and the *Protected Setup Page* section on page 97 for more detailed information.

Video Adjustment Page

The Video Setup page (FIG. 91) (*accessed by pressing the Video Adjustment button on the Setup page*) sets the Video properties of the incoming video signal from an NXA-AVB/ETHERNET Breakout Box.

FIG. 91 Video Setup page (showing default values)

The elements of the Video Setup page are described in the table below:

Video Setup Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Settings:	• The **Default Settings** button sets the video settings to their default values (indicated in this table). • The **Undo Changes** button disregards any changes made on the page since the last settings were saved. • The **Save Settings** button saves any changes made to this page.
Video Settings:	• The **Black & White** button toggles the Black & White display mode. Default = Off. • The **Sharpness** button toggles the Interpolate (Sharpness) feature. Default = Off. • The **Interlace** button toggles the Interlacing feature. Default = On.
Status:	Displays whether or not a video-sync signal is detected.
Format:	Allows you to press this blue field and cycle through a choice of available video formats (**NTSC**, **PAL**, **SECAM**, or **Auto detect**). • Default = Auto.
Brightness:	Use the UP/DN buttons to alter the brightness level of the incoming signal. • Range = 0 - 255, default = 128.
Contrast:	Use the UP/DN buttons to alter the contrast level of the incoming signal. • Range = 0 - 255, default = 128.
Saturation:	Use the UP/DN buttons to alter the color saturation level of the incoming signal. • Range = 0 - 255, default = 128.
Hue:	Use the UP/DN buttons to alter the hue level of the incoming signal. • Range = 0 - 255, default = 128.

Battery Base Page

This page (FIG. 92) allows you to alter/set the power warning preferences, monitor battery status information, and alter the display times for the battery warnings. The fields on this page are populated with information after the panel is connected to an optional NXA-BASE/1 Battery Base containing a single NXT-BP battery.

This page is ONLY available on CV10 Table Top panels (NXTs) using an NXA-BASE/1. The elements of the Battery Base page are described in the table below:

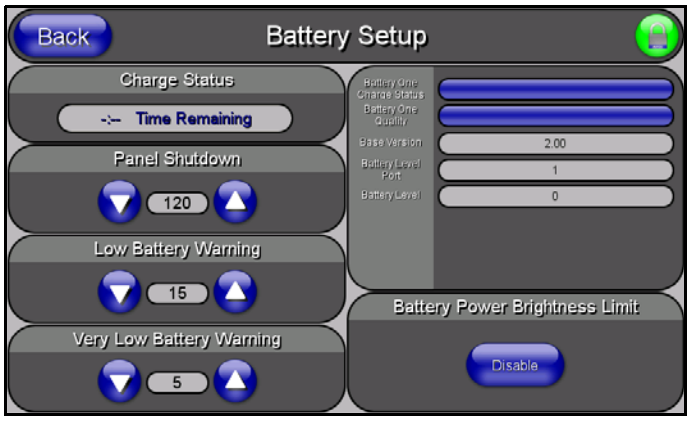


FIG. 92 Battery Base page

Battery Base Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Charge Status:	**Time Remaining** (**blue**) indicates the amount of charge time (use) remaining on the battery within the connected NXA-BASE/1. **Time Until Charged** (**green**) indicates the amount of time remaining until the battery installed within the connected NXA-BASE/1 is fully charged. • Range = 0:00 - 12:59. This is read in HH:MM, hours and minutes.
Panel Shutdown:	The **Panel Shutdown** UP/DN buttons alter the timeout value (in minutes). • This value determines the number of minutes that would need to pass before the panel automatically shuts-down. • Once shutdown, the unit would have to be restarted. A zero value disables this feature. Range = 0 - 240, default = 0 min.
Low Battery Warning:	The **Low Battery Warning** UP/DN buttons alter the time value (in minutes) available on the battery (for use) before the panel displays a low battery warning. • Range - 10 - 45, default = 15 min.
Very Low Battery Warning:	The **Very Low Battery Warning** UP/DN buttons alter the time value (in minutes) available on the battery (for use) before the panel displays a very low battery warning. This indicates a near-term panel shutdown. • Range = 3 - 15, default = 5 min. - *This value can never exceed the Low Battery Warning value.* • **When the NXT-BP battery (installed within the NXA-BASE/1 battery base) reaches a point where it needs to be recalibrated.** - A recalibration pop-up screen appears to ask whether or not you choose to recalibrate the battery at this time.

Battery Base Page Elements (Cont.)	
Battery Status fields:	This section provides the ability to monitor the current battery charge level and charge quality: • The **Battery One Charge Status** bargraph indicates the power charge available on the Slot 1 internal battery connection (bargraph range = 0 - 100). • The **Battery One Quality** bargraph indicates the physical capacity (quality) of the battery. Quality is the percentage of actual capacity vs. its rated capacity. ***For optimal performance, a battery should be replaced when the quality rating drops below 80%.*** • The **Base Version** field indicates the firmware version being used by the NXA-BASE/1 Battery Base connected to the NXT CV7 panel. • The **Battery Level Port** field indicates the port being used to report the charge status level back to the NetLinx Master on (set in TPD4). • The **Battery Level** field indicates the level being used to report the charge status level back to the NetLinx Master on (set in TPD4).
Battery Power Brightness Limit:	The DISABLE/DISABLED button acts as a power save feature with two available choices: • **Disable** - activates the brightness limit set on the Modero panel and is used to conserve battery power. Activating this feature causes the panel to function at 80% of full brightness and overrides the Panel Brightness value set on the Setup page. *This extends the battery usage time.* • **Disabled** - (*illuminated when selected*) deactivates this power save feature and makes the panel use the specified Panel Brightness level set on the Setup page.

NOTE

The term "quality" (in the context of a battery), refers to the current capacity relative to the batteries' rated capacity. For example, after constant use, a battery may be operating at 75% of its rated capacity even though it might be fully charged. In this case, the battery could be incorrectly reporting its' information back to the battery base and then consequently relating this information back to the Battery Base page. A battery can be recalibrated using an optional NXT-CHG (battery charger).

Protected Setup Navigation Buttons

The Protected Setup Navigation Buttons (FIG. 93) appear on the left of the panel screen when the Protected Setup page is currently active.

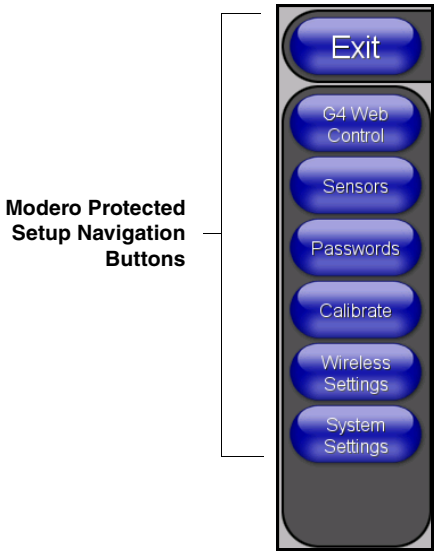


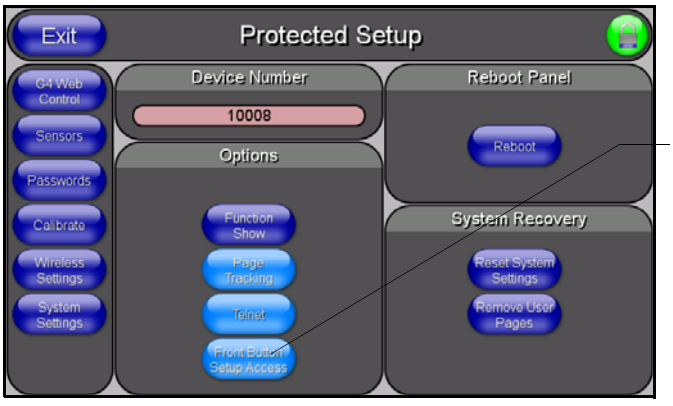
FIG. 93 Protected Setup Navigation Buttons

These Navigation Buttons are specific to these Modero panels and include panel specific elements described in the following table:

Protected Setup Navigation Button Elements	
G4 Web Control:	Press the G4 Web Control button to access the G4 Web Control page where you can enable or disable display and control of your panel (via the web) by a PC running a VNC client. • Refer to the *G4 Web Control Page* section on page 103 for more detailed information.
Sensors:	Press the Sensors button to access the Sensors Setup page where you can modify/monitor both the light and motion sensor settings. • Refer to the *Sensor Setup* section on page 105 for more detailed information.
Passwords:	Press the Passwords button to access the Passwords Setup page where you can specify up to five security passwords. *Default password is 1988.* • Refer to the *Password Setup Page* section on page 108 for more detailed information.
Calibrate:	Press the Calibrate button to access the Calibration page where you can use the displayed set of crosshairs to calibrate a touch panel. • Refer to the *Calibration Page* section on page 109 for more detailed information.
Wireless Settings:	Press the Wireless Settings button to access the Wireless Settings page where you can setup the wireless connection parameters used by the NXA-WC80211B/CF wireless interface card located within the Modero panel. • Refer to the *Wireless Settings Page* section on page 109 for more detailed information.
System Settings:	Press the System Settings button to access the System Settings page where you can alter the communication parameters of both the NetLinx Master and Modero panel. • Refer to the *System Settings Page* section on page 132 for more detailed information.

Protected Setup Page

The Protected Setup page (FIG. 94) centers around the properties used by the panel to properly communicate with the NetLinx Master. Enter the factory default password (***1988)*** into the password keypad to access this page.



Provides access to the panel firmware pages by enabling the grey front setup access button:

- Setup page (after a **3 second** press/hold)
- Calibration page (after a **6 second** press/hold)

FIG. 94 Protected Setup page-showing default values

The elements of the Protected Setup page are described in the table below:

Protected Setup Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Device Number:	Opens a keypad that is used to set and display the current device number.
Options:	Allows you to select various touch panel features: • The **Function Show** button enables the display of the channel port and channel code in the top left corner of the button, the level port and level code in the bottom left corner, and the address port and address code in the bottom right corner (see FIG. 96 for an example of the function locations). • Use the **Page Tracking** button to toggle page tracking. When enabled, the touch panel sends page data back to the NetLinx Master, or vice versa depending on the touch panel settings. • Use the **Telnet** button to enable or disable the telnet server on the panel. This feature focuses on direct telnet communication to the panel. • Use the **Front Button Setup Access** button to activate the grey Front Setup Access button (located below the LCD) to access the firmware pages. - Default condition is On. - Press and hold this grey button for **3 seconds** to access the Setup page. - Press and hold this grey button for **6 seconds** to access the Calibration page.
Reboot Panel:	Pressing this button causes the panel to restart after saving any changes.
System Recovery:	Allows you to either reset the touch panel to factory default settings and/or wipe out all existing touch panel pages: • The **Reset System Settings** button allows a user to wipe out all current configuration parameters on the touch panel (such as IP Addresses, Device Number assignments, Passwords, and other presets). - Pressing this button launches a Confirmation dialog (FIG. 95) which asks you to confirm your selection. - This dialog is configured with a delay timer that does not enable the YES button for 5 seconds. This delay provides an additional amount of time for the user to confirm their decision. • The **Remove User Pages** button allows you remove all current TPD4 touch panel pages currently on the panel (*including the pre-installed AMX Demo pages*). - Pressing this button launches a Confirmation dialog (FIG. 95) which asks you to confirm your selection. - This dialog is configured with a delay timer that does not enable the YES button for 5 seconds. This delay provides an additional amount of time for the user to confirm their decision.

Exit
Protected Setup
Confirmation Dialog
Are you sure you want to reset all system settings?
Yes
3
No
You have a wait time of 5 seconds before the YES option is enabled.

FIG. 95 Protected Setup page-System Recovery confirmation dialog

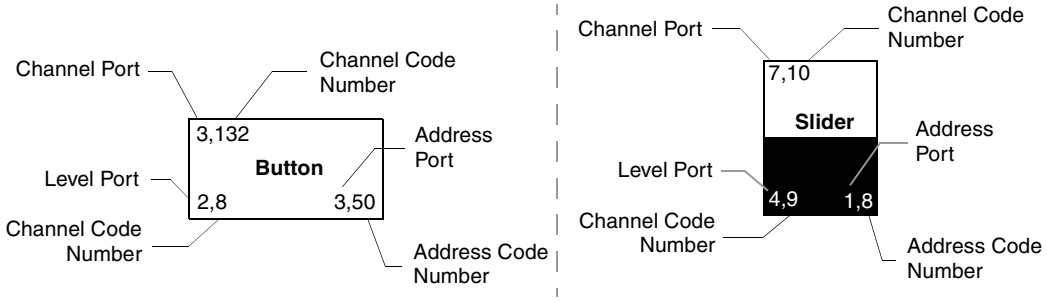


FIG. 96 Button/slider Function Show example

G4 Web Control Page

The G4 Web Control page (FIG. 97) centers around enabling and disabling both the display and control of your panel (via the web). An external PC running a VNC client (*installed during the initial communication to the G4 panel*) makes this possible.

FIG. 97 G4 Web Control page

Each panel supports the open standard Virtual Network Computing (VNC) interface. These panels contain a VNC server that allows them to accept a connection from any other device running a VNC client. Once a connection is established to that target device, the client can control the touch panel remotely.

The elements of the G4 Web Control page are described in the table below:

G4 Web Control Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
G4 Web Control Settings:	Sets the IP communication values for the touch panel and contains:
Enable/Enabled	• The Enable/Enabled button allows you to toggle between the two G4 activation settings: - **Enable** - deactivates the G4 Web Control feature on the panel. - **Enabled** - activates the G4 Web Control feature on the panel and allows an external PC running a VNC client to access the panel (*after the remaining fields are configured*).
Network Interface Select	Displays the detected method of communication to the web: • **Wired** is used when a direct Ethernet connection is being used for communication to the web. *This is a default setting if no wireless interface card is detected by the panel.* • **Wireless** is used when a wireless card is detected within the internal card slot. This method provides an indirect communication to the web via a pre-configured Wireless Access Point.
Web Control Name	Allows you to enter a unique alpha-numeric string that is used as the display name of the panel within the Manage WebControl Connections window of the new NetLinx Security browser window. • This Web Control tab displays a G4 icon alongside the link to the Web Control Name given to this panel (FIG. 98).
Web Control Password	Allows you to enter the G4 Authentication session password associated for VNC web access of this panel.
Web Control Port	Allows you to enter the port value that the VNC Web Server runs on. • Default value is 5900.
Maximum Number of Connections	This read-only field displays the maximum number of users that can be simultaneously connected to the target panel via the web. • Default value is 1.
Current Connection Count	This read-only field displays the current number of users connected to the target panel via the web. *This value cannot exceed the Maximum number field.*
G4 Web Control Timeout:	Sets the length of time (in minutes) the panel can remain idle (no cursor movements) before the session is closed and the user is disconnected. • Minimum value = 0 minutes (panel never times-out) • Maximum value = 240 minutes (panel times-out after 240 minutes/4hours)

Refer to the *Using G4 Web Control® to Interact with a G4 Panel* section on page 76 for more detailed instructions on how to use the G4 Web Control page with the new web-based NetLinx Security application.

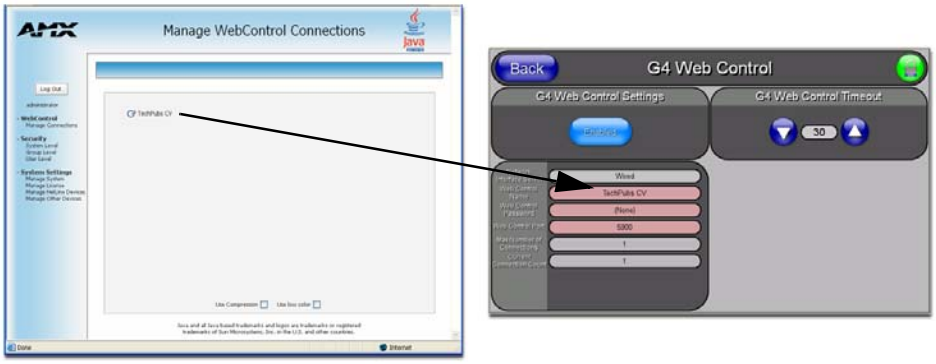


FIG. 98 Sample relationship between G4 Web Control and Mange WebControl Connections window

Sensor Setup

The Sensor Setup page (FIG. 99) allows you to adjust the Light and Motion Sensor parameters on a Modero touch panel.

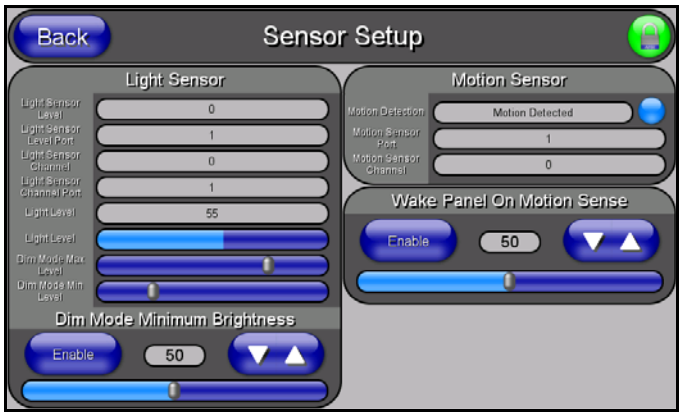


FIG. 99 Sensor Setup page

NOTE

A light level value between the Minimum and Maximum DIM Mode values delivers an average light level. The DIM mode Min Level can never exceed the DIM Mode Max Level.

The elements of the Sensor Setup page are described in the table below:

Sensor Setup Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).

Sensor Setup Page Elements (Cont.)	
Light Sensor:	Allows you to monitor and alter the sensitivity of the Modero panel light sensor: • The **Light Sensor Level** field indicates the level used to report the light sensor level back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Light Sensor Level Port** field indicates the port used to report the light sensor level back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Light Sensor Channel** field indicates the level used to report the sensor channel back to the NetLinx Master (set in TPD4). It is On when you are below the Maximum dim mode level ***(read-only)***. • The **Light Sensor Channel Port** field indicates the port used to report the sensor channel back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Light Level** field provides a numeric value representing the current value of the light level detected by the on-board photo-sensor. • The Light Level bargraph displays a horizontal bargraph indicating the current value of the light level detected by the on-board photo-sensor. This bargraph provides a visual representation of the numeric value displayed within the **Light Level** field. • Use the **Dim Mode Max Level** bargraph to alter the Maximum DIM level value used to activate the DIM Mode Brightness Level (range = 0 - 100). • Use the **Dim Mode Min Level** bargraph to alter the Minimum DIM level value used to activate the DIM Mode Brightness Level (range = 0 - 100). - The position of this bargraph can never exceed that of the Dim Mode Max Level.
Dim Mode Minimum Brightness:	Allows you to alter the sensitivity of the Modero panel light sensor: • Toggle the **Enable**/**Enabled** button to either active/inactive the DIM Mode feature: - **Enable** - activates this feature. Once active (by receiving a value below the Dim Mode Min Level value), the current light level ramps to the DIM Mode value within a few seconds. - **Enabled** - (*illuminated when selected*) deactivates this feature. • Use the **DIM Mode Brightness** UP/DN buttons to alter the DIM level. - Range = 0 - 100. - The lower the value, the darker a room must be before the LCD Brightness value changes to conform to a DIM room (and vice versa with a higher value). • The **DIM Mode Minimum Brightness** bargraph indicates the current DIM Mode Brightness level. - This level corresponds to the brightness level of the LCD used when the DIM Mode is active. - The Brightness value of the panel in a DIM room (low-light) is much less than that of a Non-DIM (well to brightly-lit) where the LCD Brightness must be higher to display the screen content clearly.
Motion Sensor:	Provides the following fields: • The **Motion Detection** field displays a reactive button that changes color (illuminates) and displays the words "Motion Detected" when motion is detected by the Modero panel's front motion sensor. • The **Motion Sensor Port** field indicates the port used to report the motion sensor channel back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Motion Sensor Channel** field indicates the channel used to report the motion sensor channel back to the NetLinx Master (set in TPD4) ***(read-only).***

Sensor Setup Page Elements (Cont.)	
Wake Panel On Motion Sense:	The Wake Panel Sensitivity relates to the sensitivity of the motion sensor to detect motion and wake the panel accordingly. • Toggle the **Enable**/**Enabled** button to either active/inactive this feature: - **Enable** - activates this feature. Activating this feature reactivates the panel from a panel timeout (sleep) mode. - **Enabled** - (*illuminated when selected*) deactivates this feature and makes the panel use the specified Display Timeout value set on the Setup Page. • Use the **Wake Panel** UP/DN buttons to alter the sensitivity value. - Range = 0 - 100. • The horizontal WAKE PANEL SENSITIVITY bargraph indicates the current motion sensitivity value associated with waking the panel from a timeout.

NOTE

There is a relationship between the motion sensor and the panel sleep feature. If a panel is set to Sleep Mode, there is a time delay before the motion sensor is activated to detect motion. By creating a time delay to the detection, this allows a user to set the sleep mode and leave the panels' detection range. In this way, the panel doesn't awake immediately after the sleep is active and you move away.

Making the most of the Automated Brightness Control feature (DIM Mode)

Please follow the steps below to set up Automated Brightness Control:

1. Set the lighting conditions in the room to maximum (turn On all the lights).
2. Set the Maximum Panel Brightness, from the Setup page, to a comfortable level.

NOTE

Sitting in front of the panel, you should be able to comfortably see someone sitting behind the panel without being "blinded" by the panel.

3. Open the Sensors Setup page (FIG. 99) from the Protected Setup menu section.
4. Move around the panel and block the direct or indirect light from the room fixtures with your body. Take note of the drop in the lighting level being detected by the panel in response to your movements.
5. Set the Maximum brightness of the Dimmer (*Dim Mode Max Level*) below the detected drop. This will make sure that the panel does not react to variations in the lighting conditions of a normal working environment.

NOTE

The maximum (upper level) of the dimmer should be at least 15% lower than the maximum detected level.

6. Set the minimum lighting conditions in the room (not complete darkness but the minimal lighting setup, unless complete darkness is an "operational option" for the room).
7. Set the Minimum Dimmer Brightness (*Dim Mode Min Level*) to a comfortable level by sitting in front of the panel. You should be able to comfortably see someone sitting behind the panel without being "blinded" by the panel.
8. Move around the panel and block the direct or indirect light from the room fixtures with your body. Take note of the drop in the lighting level being detected by the panel in response to your movements.

9. Set the Minimum brightness of the Dimmer (*Dim Mode Max Level*) below the detected drop. This will make sure that the panel does not react to variations in the lighting conditions of a normal working environment.

NOTE

The minimum (lower level) of the dimmer should be at least 10% lower than the minimum detected level (ex: lower dimmer level at 30% if the detected lighting of the room is at 40%).

Password Setup Page

The Password Setup page (FIG. 100) centers around the properties used to assign passwords for the Modero panel pages.

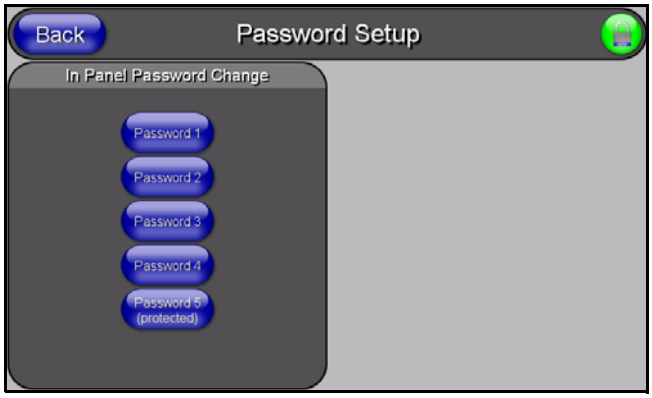


FIG. 100 Password Setup page

The elements of the Password Setup page are described in the table below:

Password Setup Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
In Panel Password Change:	Accesses the alphanumeric values associated to particular password sets. • PASSWORD 1, 2, 3, 4, 5 (protected) buttons open a keyboard where you can enter alphanumeric values associated to a selected password group. • Clearing Password #5 removes the need to enter a password before accessing the Protected Setup page.

Calibration Page

This page (FIG. 101) allows you to calibrate the touch panel using the pre-selected touch driver.

- Press and hold the grey Front Setup Access button (below the Modero LCD) for 6 seconds to access the Calibration page.
- **Press the crosshairs to calibrate the panel and return to the last active firmware page.**

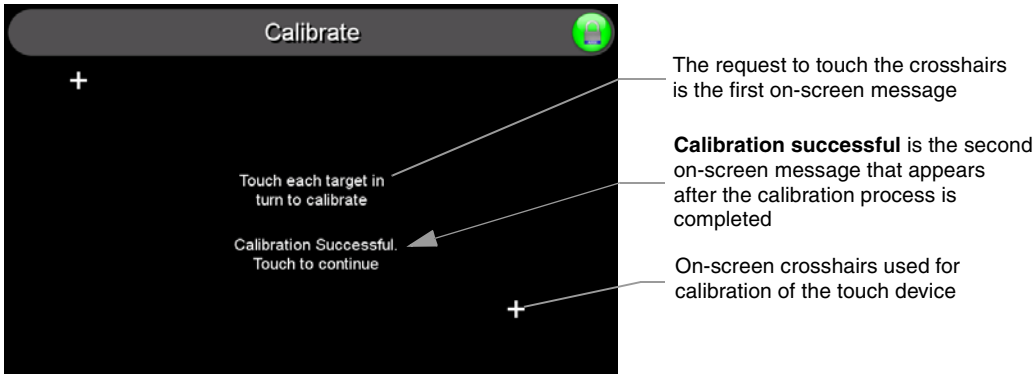

Calibrate
Touch each target in turn to calibrate
Calibration Successful. Touch to continue
The request to touch the crosshairs is the first on-screen message
Calibration successful is the second on-screen message that appears after the calibration process is completed
On-screen crosshairs used for calibration of the touch device

FIG. 101 Calibration page (actually 3 separate screens)

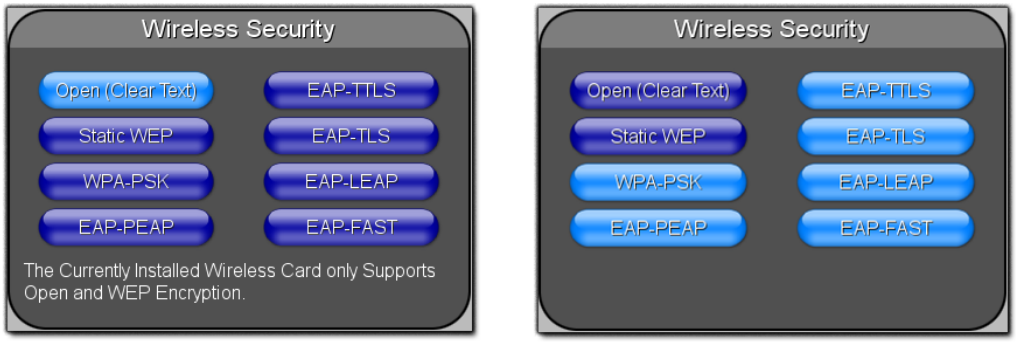
NOTE

If the calibration was improperly set and you cannot return to the Calibration page (through the panel's firmware); *you can access this firmware page via G4 WebControl where you can navigate to the Protected Setup page and press the Calibrate button through your VNC window.*
This action causes the panel to go to the Calibration page seen above, where you can physically recalibrate the actual touch panel again using the above procedures.

Wireless Settings Page

The Wireless Settings page (FIG. 103) sets the communication parameters for the installed wireless CF card (either 802.11b/g). This information includes its corresponding IP communication parameters, wireless communication settings, and read the device number assigned to the Modero panel. Both panels can use 802.11b/g for wireless communication.

Once the panel has been updated with the latest Modero firmware, some encryption and security features may/may not be supported depending on the type of wireless card being used.



802.11b wireless card **802.11g wireless card**

FIG. 102 Wireless Settings page (showing how each card supports its own security features)

Wireless Security Support	
802.11b Wi-Fi CF card:	• Open (Clear Text) • Static WEP (64-bit and 128-bit key lengths) Note: The WAP Site survey feature is disabled and is only supported by the newer 802.11g card.
802.11g Wi-Fi CF card:	• Open (Clear Text) • Static WEP (64-bit and 128-bit key lengths) • WPA-PSK • EAP security (with and without certificates) • WAP SIte Survey

Refer to the *Configuring a Wireless Connection* section on page 59 for more detailed information of setting up the Modero panel for wireless network access.

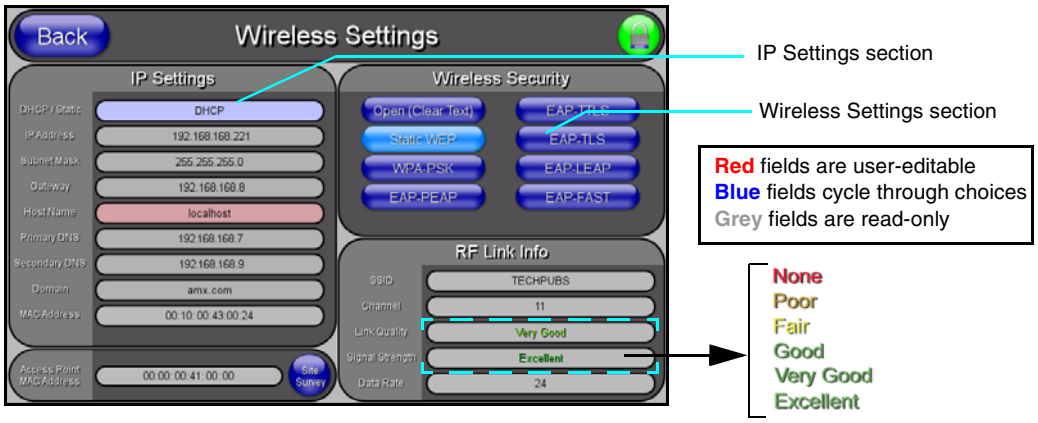


FIG. 103 Wireless Settings page (showing default values)

The elements of the Wireless Settings page are described in the table below:

Wireless Settings Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).

Wireless Settings Page Elements (Cont.)	
IP Settings:	Sets the IP communication values for the touch panel and contains:
DHCP/STATIC	Sets the panel to either DHCP or Static communication modes. • *DHCP (Dynamic Host Configuration Protocol)* assigns IP Addresses to client stations logging onto a TCP/IP network from a DHCP server. • *Static IP* is a permanent IP Address that is assigned to a node in a TCP/IP network. **Note:** If DHCP is selected, the following fields become read-only: IP Address, Subnet Mask, Gateway, Primary DNS, Secondary DNS, and Domain.
IP Address	Sets the secondary IP Address assigned to the panel.
Subnet Mask	Sets a subnetwork address to the panel. • *Subnetwork mask* is the technique used by the IP protocol to filter messages into a particular network segment (subnet).
Gateway	Sets a gateway value to the panel. • *Gateway* is a computer that either performs protocol conversion between different types of networks/applications or acts as a go-between for two or more networks that use the same protocols.
Host Name	Sets the host name of the panel. • PRIMARY DNS sets the address of the primary DNS server being used by the Modero panel for host name lookups. - *DNS (Domain Name System)* is software that lets users locate computers on a local network or the Internet (TCP/IP network) by host and domain. The DNS server maintains a database of host names for its' domain and their corresponding IP Addresses. • SECONDARY DNS sets the secondary DNS value to the panel.
Primary DNS	Sets the address of the primary DNS server used by the panel for host name lookups.
Secondary DNS	Sets the secondary DNS value to the Modero panel.
Domain	Sets the unique name on the Internet to the panel for DNS look-up.
MAC Address	This value is factory set by the manufacturer of the wireless Ethernet card.
Access Point MAC Address:	This value is factory set by the manufacturer of the Wireless Access Point (WAP). • **Site Survey** button: Clicking this button launches a page which allows a user to "sniff-out" all transmitting Wireless Access Points within the detection range of the internal NXA-WC80211GCF (*this feature is not available with the 802.11b Wi-Fi card*). The Site Survey page contains categories such as: - **Network Name (SSID**) - Wireless Access Point names - **Channel (RF)** - Channel currently being used by the WAP (Wireless Access Point) - **Security Type** - security protocol enabled on the WAP (if detectable - such as WEP, OPEN and UNKNOWN) - **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent - **MAC Address** - Unique identification of the transmitting Access Point • Refer to the *Using the Site Survey tool* section on page 61 for more detailed information on the SIte Survey page. • When communicating with a WAP200G enter the MAC Address (**BSSID**) of the target WAP as the Access Point MAC Address. Refer to the ***WAP200G*** *Instruction Manual* for more detailed information on the interaction between these two product lines.

Wireless Settings Page Elements (Cont.)	
Wireless Security:	Sets the wireless security method being used by the Modero panel to establish communication with the network (via the target WAP). • Touching any of the eight available connection method buttons launches a new connection-specific dialog page which allows the user to define the communication parameters specific to that type of connection. • Some connection methods can be chosen • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options.
Open (Clear Text)	An **Open** security method does not utilize any encryption methodology but does require that an SSID (alpha-numeric) be entered. This entry must match the Network Name (SSID) entry of the target WAP because the panel must know what device its using to bridge the communication gap between itself and the network. • Using this method causes network packets to be sent out as unencrypted text. • Pressing the **Open (Clear Text)** button opens the Open (Clear Text) Settings dialog (FIG. 104). • *The following fields are required*: *SSID*. • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options.
Static WEP	A **Static WEP** security method requires that both a target WAP be identified and an encryption method be implemented prior to establishing an active communication session. • Pressing the **Static WEP** button opens the Static WEP Settings dialog (FIG. 105). • *The following fields are required*: *SSID, Encryption method, Passphrase, WEP Key assignment, and Authentication method.* • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options.
WPA-PSK	A **WPA-PSK** security method is designed for environments where is it desirable to use WPA or WPA2 but an *802.1x authentication server is not available*. PSK connections are more secure than WEP and are simpler to configure since they implement dynamic keys but share a key between the WAP and the panel (client). • Pressing the **WPA-PSK** button opens the WPA-PSK Settings dialog (FIG. 106). • Although the button is labeled **WPA-PSK**, the encryption on the WAP could either be WPA or WPA2. The firmware in the panel will connect to the access point using the correct encryption automatically. The WPA encryption type is configured in the access point, not in the firmware. • WAPs do not show WPA or WPA2 on their configuration screens. - *WPA* is normally displayed on an WAP as *TKIP*. - *WPA2* is normally displayed on an WAP as *AES CCMP*. • *The following fields are required*: *SSID and Password/Pass Phrase*. - The values that need to be entered are the SSID of the WAP and a pass phrase that is a minimum of 8 characters and a maximum of 63. - The exact same pass phrase including capitalization must be entered in the access point. - Whenever entering a password on any screen, touch the password field to pop up the keyboard, press **Clear** to completely erase the previous password, and then enter the new password. • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options.

Wireless Settings Page Elements (Cont.)	
Wireless Security (Cont.):	
EAP-PEAP	An **EAP-PEAP** security method is designed for wireless environments where its necessary to securely transmit data over a wireless network. • Pressing the **EAP-PEAP** button opens the EAP-PEAP Settings dialog (FIG. 111). • *The following fields are required*: *SSID, Identity, Password, PEAP Version, and Inner Authentication Type* • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options. • For more information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 203.
EAP-TTLS	An **EAP-TTLS** security method is designed for wireless environments where its necessary to first have the Radius server directly validate the identity of the client (panel) before allowing it access to the network. This validation is done by tunneling a connection through the WAP and directly between the panel and the Radius server. By initially keeping the network out of the picture, there is far more security validation going on behind the scenes before any possible access to the network is granted to the client. Once the client is identified and then validated, the Radius server disconnects the tunnel and allows the panel to access the network directly via the target WAP. • Pressing the **EAP-TTLS** button opens the EAP-TTLS Settings dialog (FIG. 112). • *The following fields are required*: *SSID, Identity, Password, and Inner Authentication Type* • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options. • For more information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 203.
EAP-TLS	An **EAP-TLS** security method is designed for wireless environments where its necessary to securely transmit data over a wireless network by adding an additional level of security protocol via the use of a private key. • Pressing the **EAP-TLS** button opens the EAP-TLS Settings dialog (FIG. 113). • *The following fields are required*: *SSID, Identity, Client Certificate, Private Key, and Private Key password* • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options. • For more information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 203.
EAP-LEAP	An **EAP-LEAP** security method is designed for wireless environments where its not required to have both a client or server certificate validation scheme in place yet necessary to securely transmit data over a wireless network. • Pressing the EAP-LEAP button opens the EAP-LEAP Settings dialog (FIG. 107). • *The following fields are required*: *SSID, Identity, and Password* • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options.

Wireless Settings Page Elements (Cont.)	
Wireless Security (Cont.):	
EAP-FAST	An **EAP-FAST** security method is designed for wireless environments where both security and ease of setup are balanced together. • Pressing the EAP-FAST button opens the EAP-FAST Settings dialog (FIG. 109). • *The following fields are required*: *SSID, Identity, Anonymous Identity, and Password* • Refer to the following *Wireless Settings Page - Security Options - Overview* section on page 115 for further details on these security options.
Site Survey:	The Site Survey tool allows installers to see all of the WAPs within the panel's communication/detection area. • The information displayed includes: SSID, Channel, Signal Strength, Security Type (if detectable), and MAC address of the WAP. • From the site survey tool, a user can then select and connect to a WAP although proper configuration of the security settings may still be required. • Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature.
RF Link Info:	Sets the communication values for the internal wireless interface card.
SSID	Displays the currently used SSID of the target WAP.
Channel	The RF channel being used for connection to the WAP (***read -only***). • This is determined through the WAP.
Link Quality	Displays the current quality of the link (*as descriptive colored text*) from the wireless NIC to the Wireless Access Point in real time. • The bargraph has been replaced with a descriptions: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent**. *Green color text indicates better communication quality.* • It reports the quality of the signal over the air (direct sequence spread spectrum). Even when the link quality is at its lowest you still have a connection and with it the ability to transmit and receive data, even if at much lower speeds. **Note:** Both Link Quality and Signal Strength are applicable to the RF connection only. It is quite possible to have an RF signal to a Wireless Access Point but be unable to communicate with it because of either incorrect IP or encryption settings.
Signal Strength	SNR (Signal Noise Ratio) is a measure of the relative strength of a wireless RF connection. This indicator displays a description of the signal strength from the Wireless Access Point connection. • The bargraph has been replaced with a descriptions: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent**. *Green color text indicates better signal strength.* • Given this value and the link quality above, a user can determine the noise level component of SNR. Ex: If the signal strength is high but the link quality is low then the cause of the link degradation is noise. However, if the signal strength is low and the link quality is low the cause would simply be signal strength.
Data Rate	The data rate (in Mbps) at which the panel is currently communicating with a target WAP at (dynamic). • As you move closer to the target WAP (and both the signal strength/quality), the data rate increases and as the quality degrades this rate decreases. • Data rates for 802.11b communication are: 1, 2, 5.5, and 11 Mbps. • Ex: 802.11b has a max data rate is 11 Mbps.

Wireless Settings Page - Security Options - Overview

The Wireless Settings page allows a user to select from up to eight available wireless security methods now available via the NXA-WC80211GCF Wi-Fi card. The new security methods incorporate the following security technology: **WPA**, **WPA2**, and **EAP** (some of which require the upload of unique certificate files to a target panel). Refer to the *Appendix B - Wireless Technology* section on page 197 for more further information.

Wireless Settings Page - Security Options - Open (Clear Text)

An **Open** security method does not utilize any encryption methodology but does require that an SSID (alpha-numeric) be entered. Using this method causes network packets to be sent out as unencrypted text. Refer to the *Configuring a Wireless Connection* section on page 59 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Pressing the **Open (Clear Text)** button opens the Open (Clear Text) Settings dialog.

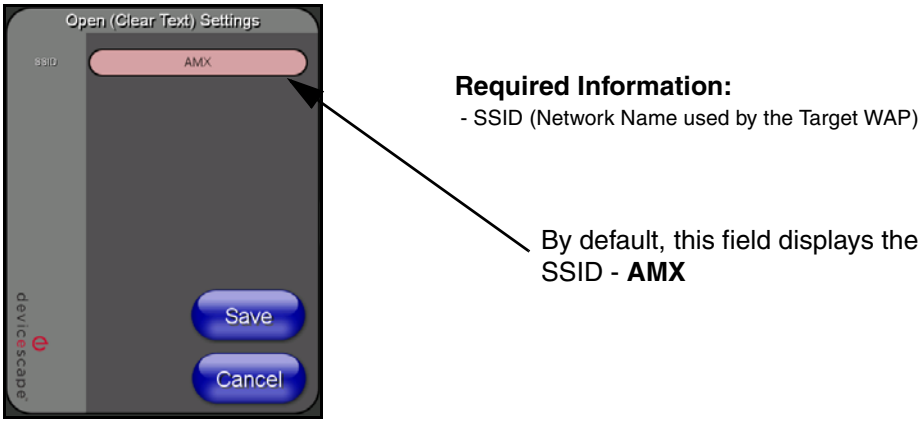
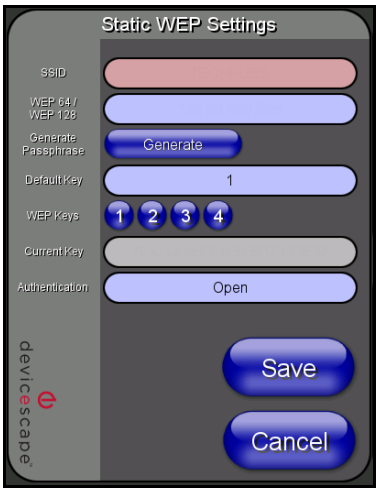


FIG. 104 Wireless Settings page - Open (Clear Text) security method

Wireless Security - Open (Clear Text) Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • From the *Network Name (SSID)* keyboard, enter the SSID name used on your target Wireless Access Point (case sensitive). - The card should be given the SSID used by the target WAP. - If this field is left blank, the unit will attempt to connect to the first available WAP. By default, all WAP200Gs use **AMX** as their assigned SSID value. • One of the most common problems associated with connection to a WAP arise because the SSID was not entered properly. You must maintain the same case when entering the SSID information. ABC is not the same as Abc. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information.
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

Wireless Settings Page - Security Options - Static WEP

A Static WEP security method requires that both a target WAP be identified and an encryption method be implemented prior to establishing an active communication session. In addition to providing both Open and Shared Authentication capabilities, this page also supports Hexadecimal and ASCII keys. Refer to the *Configuring a Wireless Connection* section on page 59 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Pressing the **Static WEP** button opens the Static WEP Settings dialog (FIG. 105).



Required Information:

- SSID (Network Name used by the Target WAP)
- Encryption Method
- Passphrase
- WEP Key assignment
- Authentication Method

FIG. 105 Wireless Settings page - Static WEP security method

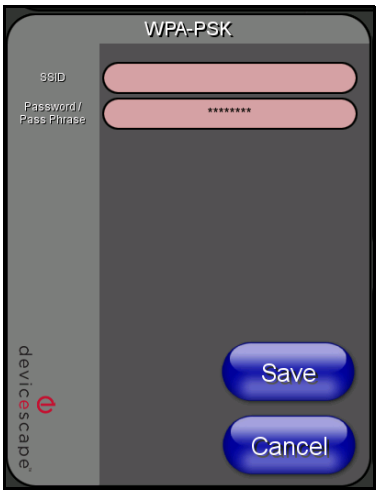
Wireless Security - Static WEP Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information.
WEP 64 / WEP 128:	Cycles through the available encryption options: *64 Bit Key Size or 128 Bit Key Size*. Wired Equivalent Privacy is an 802.11 security protocol for wireless networks. The WEP encryption method is designed to provide the "equivalent" security available as in wireline networks. • **WEP64** enables WEP encryption using a 64 Bit Key Size. In this case all packets will be transmitted with their contents encrypted using the Default WEP Key. • **WEP128** enables WEP encryption using a 128 Bit Key Size. All packets are transmitted with their contents encrypted using the Default WEP Key. • If the key is not the correct size, the system will resize it to match the number of bits required for the WEP encryption mode selected.

Wireless Security - Static WEP (Cont.)	
Generate (Passphrase):	Pressing the **Generate** button displays an on-screen keyboard which allows you to enter a passphrase and then AUTOMATICALLY generate all four WEP keys which are compatible only among Modero panels. • **Note:** The code key generator on Modero panels use the same key generation formula. Therefore, this same Passphrase generates identical keys when done on any Modero because they all use the same Modero-specific generator. The Passphrase generator is case sensitive. • Take these WEP keys and enter them into the target WAP. When also working with multiple panels, these WEP Keys (*identical across all Modero panels*) must be entered manually into the target WAP. • Once all panels have been setup in this way, these WEP keys can then be entered into the associated Wireless Access Point for ease of installation. • The Passphrase generator is unique to Modero panels. The Key generator on these Modero panels are specific and do not generate the same keys as other external non-AMX wireless devices. - Example: If you enter the word **apple** into the Passphrase generator on a 3rd-party Wireless Access Point, it comes back with 1a:2b:3c:4d:etc. Entering the same **apple** in the Passphrase generator of any Modero panel generates a different key: a1:b2:c3:d4:etc. Only AMX Modero panels generate **the same** Current Key by using a unique Passphrase key generation technology. A Current Key string, when generated anywhere else, will not match those created on the Modero panels. **Note:** The code key generator on Modero panels use the same key generation formula. The passphrase generator is case sensitive.
Default Key:	Cycles through the four available WEP key identifiers in order to select a WEP key to use. *As the Default Key value is altered (through selection) the corresponding Current Key is displayed. Each of these corresponds to a WEP key.* • This feature is useful for accessing different networks without having to re-enter that networks' WEP key. • It is also sometimes used to set up a rotating key schedule to provide an extra layer of security.
WEP Keys:	This feature provides you with another level of security by selecting a Key value. Both ASCII and HEX keys are supported. • A single button is available for each WEP key up to a maximum of four keys. • Pushing any of these buttons brings up an on-screen keyboard. Keys should be entered in hexadecimal notation. It is common practice for every two characters (representing a single byte) to be separated by a colon. • Since both ASCII and HEX keys are supported it is important to note that up to four keys can be configured for both. *- An ASCII key utilizes either 5 or 13 ASCII characters* *- A HEX key utilizes either 10 or 26 Hexidecimal characters* • Press **Done** to accept any changes and save the new value. • **Ex: 01:0A:67:F3:56**, although this is not necessary and the key may be entered by omitting the colons. A 64-bit key will be 10 characters in length while a 128-bit key will be 26 characters in length. The length of the key entered determines the level of WEP encryption employed. Either 64-bit or 128-bit. • 128-bit keys may also be entered and are used if supported by the internal wireless card.

Wireless Security - Static WEP (Cont.)	
Current Key:	Displays the current WEP key in use. Keys may also be examined by touching the key buttons and noting the keyboard initialization text. • When working with a single panel and a single WAP, it is recommended that you manually enter the Current Key from the WAP into the selected WEP Key. • When working with a single WAP and multiple panels, it is recommended that you generate a Current Key using the same passphrase on all panels and then enter the panel-produced WEP key manually into the Wireless Access Point. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored key information.
Authentication:	Toggles between the two authentication modes: *Open + WEP* or *Shared + WEP*: The choice here is whether or not the SSID is broadcast publicly or encrypted. • An *Open system + WEP* network allows connections from any client without authenticating whether that client has permission to associate with the network. • A *Shared key + WEP* network requires the client to submit a key which is shared by the network Wireless Access Point before it is given permission to associate with the network. ***In this case the key is the same as the WEP encryption key***. • In both cases, even after association has taken place, if WEP encryption has also been enabled then the client will still require the WEP key to encrypt and decrypt packets in order to communicate successfully with the network.
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

Wireless Settings Page - Security Options - WPA-PSK

A WPA-PSK security method is designed for environments where its desirable to use WPA or WPA2 but an 802.1x authentication server is not available. PSK connections are more secure than WEP and are simpler to configure since they implement dynamic keys but share a key between the WAP and the panel (client). Refer to the *Configuring a Wireless Connection* section on page 59 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Pressing the **Static WEP** button opens the Static WEP Settings dialog (FIG. 106).



Required Information:
- SSID (Network Name used by the Target WAP)
- Password/Pass Phrase

FIG. 106 Wireless Settings page - WPA-PSK security method

Wireless Security - WPA-PSK Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information.
Password/Pass Phrase:	When pressed, the panel displays an on-screen keyboard which allows you to enter a passphrase (password). • This alpha-numeric string must use a minimum of 8 characters and a maximum of 63. Note: The exact pass phrase string (including capitalization) must be entered on the target WAP. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored passwords.
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

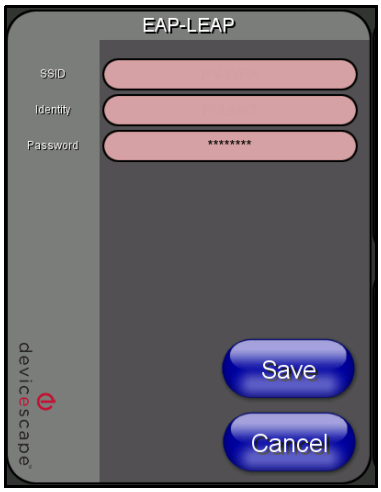
Wireless Settings Page - Security Options - EAP-LEAP

EAP (Extensible Authentication Protocol) is a Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. Most of the configuration fields described below take variable length strings as inputs. Whenever these fields are selected, an on-screen keyboard appears which allows the string to then be entered.

LEAP (Lightweight Extensible Authentication Protocol) was developed by Cisco© Systems as a way to securely transmit authentication information over a wireless network environment.
LEAP **does not use** client (panel) or server (RADIUS) certificates and is therefore one of the least secure EAP security methods but can be utilized successfully by implementing sufficiently complex passwords.

An EAP-LEAP security method is designed for wireless environments where its not required to have both a client or server certificate validation scheme in place yet necessary to securely transmit data over a wireless network. Refer to the *EAP Authentication* section on page 201 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Refer to FIG. 108 for an example of what a typical EAP-LEAP system configuration page would like.

Pressing the **EAP-LEAP** button opens the EAP-LEAP Settings dialog (FIG. 107).



Required Information:

- SSID (Network Name used by the Target WAP)
- Identity (similar to the Username used for network access)
- Password (similar to the Password used for network access)

FIG. 107 Wireless Settings page - EAP-LEAP security method

Wireless Security - EAP-LEAP Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information. • Note: In all cases, the SSID of the WAP must be entered. If it is left blank, the panel will try to connect to the first access point which can be found that supports EAP. In this situation however, a successful connection is not guaranteed because the identified WAP may be connected to a RADIUS server which does not support the specified EAP type and/or may not have the proper user identities configured.
Identity:	When pressed, the panel displays an on-screen keyboard which allows you to enter an EAP Identity string which is how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Note: Typically, this is in the form of a username such as: jdoe@amx.com • Use the on-screen keyboard's **Clear** button to completely erase any previously stored identity/username information.
Password:	When pressed, the panel displays an on-screen keyboard which allows you to enter the network password string specified for the user entered within the *Identity* field. This is also how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to the password entered to gain access to a secured workstation. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored passwords.

Wireless Security - EAP-LEAP Settings (Cont.)	
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

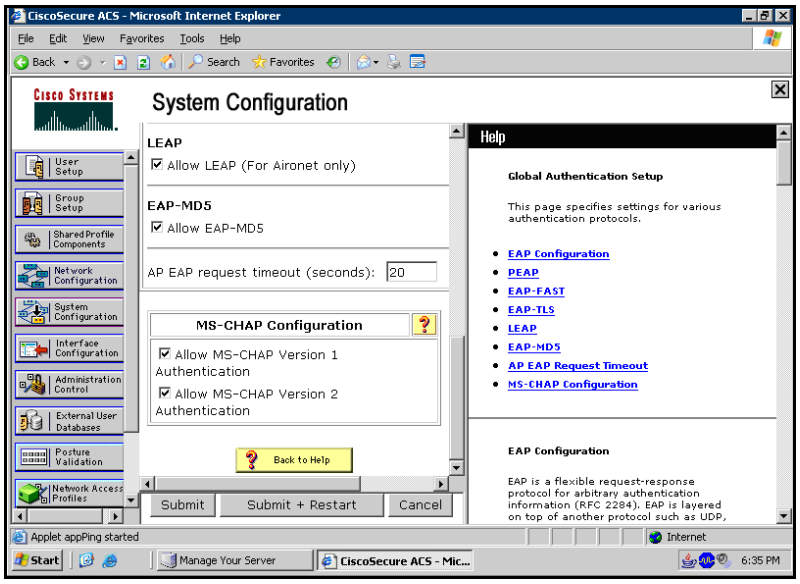


FIG. 108 EAP-LEAP sample Cisco System Security page

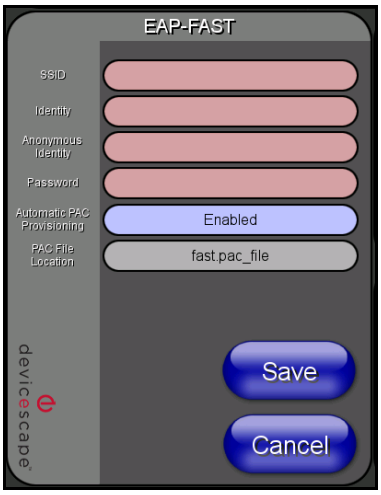
Wireless Settings Page - Security Options - EAP-FAST

EAP (Extensible Authentication Protocol) is a Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. Most of the configuration fields described below take variable length strings as inputs. Whenever these fields are selected, an on-screen keyboard appears which allows the string to then be entered.

FAST (Flexible Authentication via Secure Tunneling) was developed by Cisco© Systems and has been described as being as secure as PEAP while being as easy to setup as LEAP.

EAP-FAST does use a certificate file, however, it can be configured to download that certificate automatically the first time that the panel tries to authenticate itself. Automatic certificate downloading is more convenient but slightly less secure since its the certificate which is transferred wirelessly and could then be sniffed-out.

An EAP-FAST security method is designed for wireless environments where both security and ease of setup are balanced together. Refer to the *EAP Authentication* section on page 201 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Pressing the **EAP-FAST** button opens the EAP-FAST Settings dialog (FIG. 109).



Required Information:

- SSID (Network Name used by the Target WAP)
- Identity (similar to the Username used for network access)
- Anonymous Identity (similar to a fictitious call-sign)
- Password (similar to the Password used for network access)

FIG. 109 Wireless Settings page - EAP-FAST security method

Wireless Security - EAP-FAST Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information. • Note: In all cases, the SSID of the WAP must be entered. If it is left blank, the panel will try to connect to the first access point which can be found that supports EAP. In this situation however, a successful connection is not guaranteed because the identified WAP may be connected to a RADIUS server which does not support the specified EAP type and/or may not have the proper user identities configured.
Identity:	When pressed, the panel displays an on-screen keyboard which allows you to enter an EAP Identity string which is how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Note: Typically, this is in the form of a username such as: jdoe@amx.com • Use the on-screen keyboard's **Clear** button to completely erase any previously stored identity/username information.
Anonymous Identity:	When pressed, the panel displays an on-screen keyboard which allows you to enter an IT provided alpha-numeric string which is similar to the username used as the identity but does not represent a real user. • This information is used as a fictitious name which might be seen by wireless preying eyes (such as sniffer programs) during the initial connection and setup process between the panel and the Radius server. In this way the real identity (username) will never be seen by anyone. Note: Typically, this is in the form of a fictitious username such as: anonymous@amx.com • Use the on-screen keyboard's **Clear** button to completely erase any previously stored identity/username information.

Wireless Security - EAP-FAST Settings (Cont.)	
Password:	When pressed, the panel displays an on-screen keyboard which allows you to enter the network password string specified for the user entered within the Identity field. This is also how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to the password entered to gain access to a secured workstation. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored passwords.
Automatic PAC Provisioning:	This selection presents a binary choice as to whether or not Protected Access Credential provisioning is enabled or disabled. • When pressed, this field toggles between: **Enabled** *(automatic)* or **Disabled** *(manual)*. • If **Enabled** is selected, the following *PAC File Location* field is then greyed-out because the search for the PAC file is automatically done. • If **Disabled** is selected, the user is required to manually locate a file containing the PAC shared secret credentials for use in authentication. **In this case, the IT department must create a PAC file and then transfer it into the panel using the AMX Certificate upload application.**
PAC File Location:	This field is used when the previous Automatic PAC Provisioning option has been **Disabled**. • When pressed, the panel displays an on-screen PAC File Location keyboard which allows you to enter the name of the file containing the PAC shared secret credentials for use in authentication. • This field is only valid when the automatic PAC provisioning feature has been enabled via the previous field.
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

NOTE

REGARDING AUTOMATIC PROVISIONING:
Even when automatic provisioning is enabled, the PAC certificate is only downloaded the first time that the panel connects to the RADIUS server. This file is then saved into the panel's file system and is then reused from then on. It is possible for the user to change a setting (such as a new Identity) that would invalidate this certificate. In that case, the panel must be forced to download a new PAC file.
*To do this, set Automatic PAC Provisioning to **Disabled** and then back to **Enabled**. This forces the firmware to delete the old file and request a new one.*

EAP Security's Using Server Certificates - Overview

The following EAP types all support a server certificate:

- EAP-PEAP
- EAP-TTLS
- EAP-TLS

All three of these certificate-using security methods are documented in the following sections. EAP Authentication goes a step beyond just encrypting data transfers, but also requires that a set of credentials be validated before the client (panel) is allowed to connect to the rest of the network (FIG. 110). Below is a description of this process. It is important to note that there is no user intervention necessary during this process. It proceeds automatically based on the configuration parameters entered into the panel.

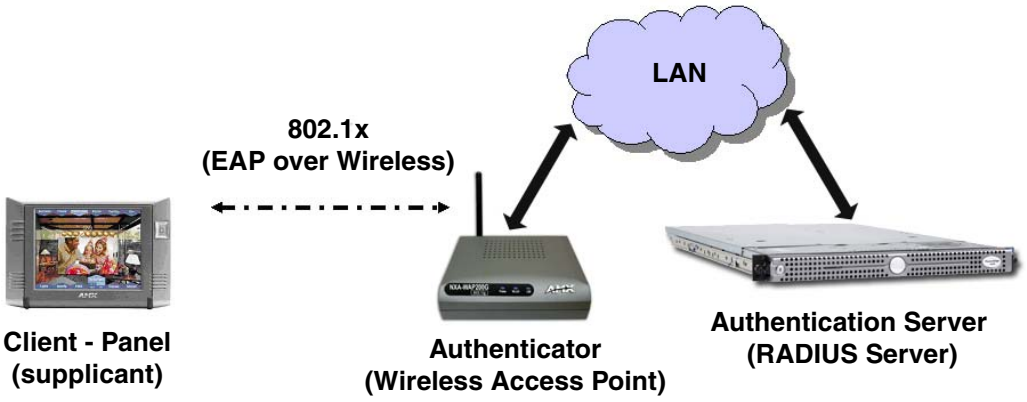


FIG. 110 EAP security method in process

A server certificate file uses a certificate that is installed in a panel so that the RADIUS server can be validated before the panel tries to connect to it. The field name associated with this file is *Certificate Authority.*

If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. The most secure connection method uses a server certificate.

If no server certificate will be used then, this field should be left blank. If the field contains a file name, then a valid certificate file with the same file name must be previously installed on the panel. Otherwise the authentication process will fail.

Wireless Settings Page - Security Options - EAP-PEAP

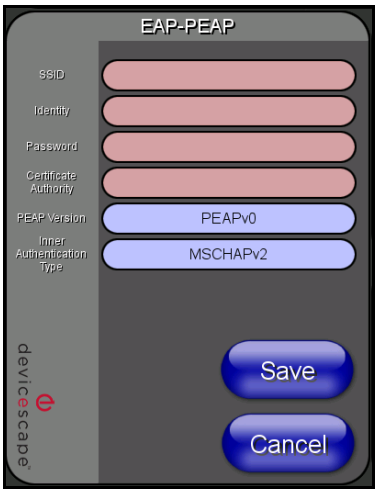
EAP (Extensible Authentication Protocol) is a Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. Most of the configuration fields described below take variable length strings as inputs. Whenever these fields are selected, an on-screen keyboard appears which allows the string to then be entered.

PEAP (Protected Extensible Authentication Protocol) was developed by both Cisco© Systems and Microsoft® as a way to securely transmit authentication information, such as passwords, over a wireless network environment. PEAP uses only server-side public key certificates and therefore does not need a client (panel) certificate which makes the configuration and setup easier.

There are two main versions of the PEAP protocol supported by panel's Devicescape Wireless Client are:

- **PEAPv0** (developed with Microsoft)
- **PEAPv1** (developed exclusively by Cisco)
- PEAP uses an inner authentication mechanism which is supported by the Devicescape Wireless Client, the most common of which are:
  - **MSCHAPv2** with PEAPv0 and
  - **GTC** with PEAPv1

An EAP-PEAP security method is designed for wireless environments where its necessary to securely transmit data over a wireless network. Refer to the *EAP Authentication* section on page 201 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Pressing the **EAP-PEAP** button opens the EAP-PEAP Settings dialog (FIG. 111).



Required Information:
- SSID (Network Name used by the Target WAP)
- Identity (similar to the Username used for network access)
- Password (similar to the Password used for network access)
- PEAP Version (PEAPv0, PEAPv1, or PEAPv1 w/ peaplabel=1)
- Inner Authentication Type (supported by the Devicescape)

FIG. 111 Wireless Settings page - EAP-PEAP security method

Wireless Security - EAP-PEAP Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information. Note: In all cases, the SSID of the WAP must be entered. If it is left blank, the panel will try to connect to the first access point which can be found that supports EAP. In this situation however, a successful connection is not guaranteed because the identified WAP may be connected to a RADIUS server which does not support the specified EAP type and/or may not have the proper user identities configured.

Wireless Security - EAP-PEAP (Cont.)	
Identity:	When pressed, the panel displays an on-screen keyboard which allows you to enter an EAP Identity string which is how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Note: Typically, this is in the form of a username such as: jdoe@amx.com • Use the on-screen keyboard's **Clear** button to completely erase any previously stored identity/username information.
Password:	When pressed, the panel displays an on-screen keyboard which allows you to enter the network password string specified for the user entered within the Identity field. This is also how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to the password entered to gain access to a secured workstation. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored passwords.
Certificate Authority:	When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate. This field is optional. If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
PEAP Version:	When pressed, this field cycles through the choices of available PEAP: **PEAPv0, PEAPv1,** or **PEAPv1 w/peaplabel=1**.
Inner Authentication Type:	When pressed, this field cycles through the choices of available Inner Authentication mechanisms supported by the Devicescape Secure Wireless Client. The most commonly used are: **MSCHAPv2** and **GTC**. • MSCHAPv2 (*used with PEAPv0*) • TLS • GTC (*used with PEAPv1*) • OTP • MD5-Challenge
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

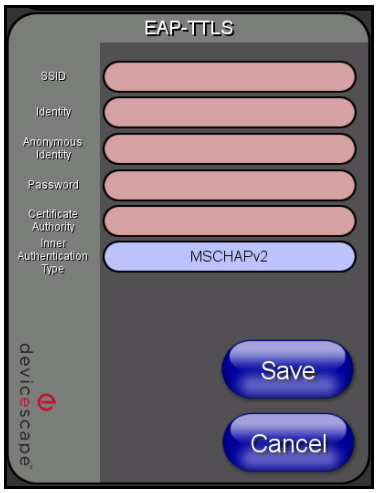
Wireless Settings Page - Security Options - EAP-TTLS

EAP (Extensible Authentication Protocol) is a Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. Most of the configuration fields described below take variable length strings as inputs. Whenever these fields are selected, an on-screen keyboard appears which allows the string to then be entered.

TTLS (EAP Tunneled Transport Layer Security) was an authentication method, like PEAP, that does not use a client certificate to authenticate the panel. This method is more secure than PEAP in that it does not broadcast the identity of the user. The setup, although similar to PEAP, differs in the following areas:

- An anonymous identity MUST be specified until the secure tunnel between the panel and the Radius server is setup to transfer the real identity of the user.
- There is no end-user ability to select from the different types of PEAP.
- Additional Inner Authentication choices are available to the end-user.

An EAP-TTLS security method is designed for wireless environments where its necessary to first have the Radius server directly validate the identity of the client (panel) before allowing it access to the network. This validation is done by tunneling a connection through the WAP and directly between the panel and the Radius server. By initially keeping the network out of the picture, there is far more security validation going on behind the scenes before any possible access to the network is granted to the client. Once the client is identified and then validated, the Radius server disconnects the tunnel and allows the panel to access the network directly via the target WAP. Refer to the *EAP Authentication* section on page 201 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Pressing the **EAP-TTLS** button opens the EAP-TTLS Settings dialog (FIG. 112).



Required Information:

- SSID (Network Name used by the Target WAP)
- Identity (similar to the Username used for network access)
- Password (similar to the Password used for network access)
- Inner Authentication Type (supported by Devicescape)

FIG. 112 Wireless Settings page - EAP-TTLS security method

Wireless Security - EAP-TTLS Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information. • Note: In all cases, the SSID of the WAP must be entered. If it is left blank, the panel will try to connect to the first access point which can be found that supports EAP. In this situation however, a successful connection is not guaranteed because the identified WAP may be connected to a RADIUS server which does not support the specified EAP type and/or may not have the proper user identities configured.

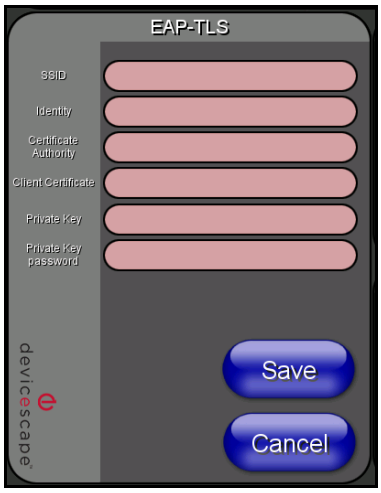
Wireless Security - EAP-TTLS Settings (Cont.)	
Identity:	When pressed, the panel displays an on-screen keyboard which allows you to enter an EAP Identity string which is how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Note: Typically, this is in the form of a username such as: jdoe@amx.com • Use the on-screen keyboard's **Clear** button to completely erase any previously stored identity/username information.
Anonymous Identity:	When pressed, the panel displays an on-screen keyboard which allows you to enter an IT provided alpha-numeric string which is similar to the username used as the identity but does not represent a real user. • This information is used as a fictitious name which might be seen by wireless preying eyes (such as sniffer programs) during the initial connection and setup process between the panel and the Radius server. In this way the real identity (username) will never be seen by anyone. Note: Typically, this is in the form of a fictitious username such as: anonymous@amx.com • Use the on-screen keyboard's **Clear** button to completely erase any previously stored identity/username information.
Password:	When pressed, the panel displays an on-screen keyboard which allows you to enter the network password string specified for the user entered within the Identity field. This is also how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to the password entered to gain access to a secured workstation. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored passwords.
Certificate Authority:	When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate. This field is optional and can be left blank. If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Inner Authentication Type:	When pressed, this field cycles through the choices of available Inner Authentication mechanism supported by the Devicescape Secure Wireless Client: • MSCHAPv2 (*default because its the most common*) • MSCHAP • PAP • CHAP • EAP-MSCHAPv2 • EAP-GTC • EAP-OTP • EAP-MD5-Challenge
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

Wireless Settings Page - Security Options - EAP-TLS

EAP (Extensible Authentication Protocol) is a Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. Most of the configuration fields described below take variable length strings as inputs. Whenever these fields are selected, an on-screen keyboard appears which allows the string to then be entered.

TLS (Transport Layer Security) was the original standard wireless LAN EAP authentication protocol. TLS requires additional work during the deployment phase but provides additional security since even a compromised password is not enough to break into an EAP-TLS protected wireless network environment.

An EAP-TLS security method is designed for wireless environments where its necessary to securely transmit data over a wireless network by adding an additional level of security protocol via the use of a private key. Refer to the *EAP Authentication* section on page 201 for further details on these security options. Refer to the *Using the Site Survey tool* section on page 61 for more information on using this feature. Pressing the **EAP-TLS** button opens the EAP-TLS Settings dialog (FIG. 113).



Required Information:

- SSID (Network Name used by the Target WAP)
- Identity (similar to the Username used for network access)
- Client Certificate file (validates client (panel))
- Private Key and Private Key Password

FIG. 113 Wireless Settings page - EAP-TLS security method

Wireless Security - EAP-TLS Settings	
SSID (Service Set Identifier):	The SSID is the unique name used on the WAP and then assigned to all panels in a wireless network that are communicating to the same target WAP. • This is required by the WAP before the panel is permitted to join the wireless network. • It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. • This unique string identifies the network and is the same string for all users on the same network. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored SSID information. • Note: In all cases, the SSID of the WAP must be entered. If it is left blank, the panel will try to connect to the first access point which can be found that supports EAP. In this situation however, a successful connection is not guaranteed because the identified WAP may be connected to a RADIUS server which does not support the specified EAP type and/or may not have the proper user identities configured.

Wireless Security - EAP-TLS Settings (Cont.)	
Identity:	When pressed, the panel displays an on-screen keyboard which allows you to enter an EAP Identity string which is how the panel identifies itself to the Authentication (RADIUS) Server. • This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Note: Typically, this is in the form of a username such as: jdoe@amx.com • Use the on-screen keyboard's **Clear** button to completely erase any previously stored identity/username information.
Certificate Authority:	When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate. The Certificate authority is optional but the client certificate is required. If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Client Certificate:	When pressed, the panel displays an on-screen Client Certificate File Location keyboard which allows you to enter the name of the file containing the client (panel) certificate for use in certifying the identity of the client (panel). • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information. • Refer to the following *Client certificate configuration* section for more information regarding Client Certificates and their parameters.
Private Key:	When pressed, the panel displays an on-screen Client Private Key File Location keyboard which allows you to enter the name of the file containing the private key. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Private Key password:	This field should only be used if the Private Key is protected with a password. If there is no password protection associated with the Private Key, then this field should be left ***blank***. • When pressed, the panel displays an on-screen Private Key Password keyboard which allows you to enter an alpha-numeric password string. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Save/Cancel:	• Use the **Save** button to store the new security information, incorporate it, and then return to the previous Wireless Settings page. • Use the **Cancel** button to cancel any updates to the security parameters and return to the previous Wireless Settings page.

Client certificate configuration

There are several ways in which a client certificate can be configured by an IT department. The client certificate and private key can both be incorporated into one file or split into two separate files. In addition, the file format used by these files could be PEM, DER, or PKCS12. These formats are described later in this section. The following table describes how to fill in the fields for each possible case.

Client Certificate Configuration

Certificate Configuration	Client Certificate Field	Private Key Field
Single file contains both the client certificate and private key. Format is: **PEM** or **DER**.	Enter the file name	Enter the same file name
First file contains the client certificate and the second file contains the private key. Format is: **PEM** or **DER**.	Enter the first file name	Enter the second file name
Single file contains both the client certificate and the private key. Format is: **PKCS12**	Leave this field blank	Enter the file name
First file contains the client certificate and the second file contains the private key. Format is: **PKCS12**	This configuration is not supported	This configuration is not supported

AMX supports the following security certificates within three different formats:

- **PEM** (Privacy Enhanced Mail)
- **DER** (Distinguished Encoding Rules)
- **PKCS12** (Public Key Cryptography Standard #12)

PKCS12 files are frequently generated by Microsoft certificate applications. Otherwise, PEM is more common.

Certificate files frequently use 5 file extensions. It can be confusing because there is not a one to one correspondence. The following table shows the possible file extension used for each certificate type:

Certificates and their Extensions

Certificate Type	Possible File Extensions
PEM	.cer .pem .pvk
DER	.cer .der
PKCS12	.pfx

It is important to note which certificate types are supported by the different certificate fields used on the configuration screens (PEAP, TTLS, and TLS). The following table outlines the firmware fields and their supported certificate types.

Certificate Types Supported by the Modero Firmware	
Configuration Field Name	Certificate File Type Supported
Certificate Authority field	PEM and DER
Client Certificate field	PEM and DER
Private Key field	.PEM, DER, and PKCS12

System Settings Page

The System Settings page (FIG. 114) sets the Secondary DNS Address information with its corresponding IP communication parameters, NetLinx Master communication settings, and reads the device number assigned to the Modero panel.

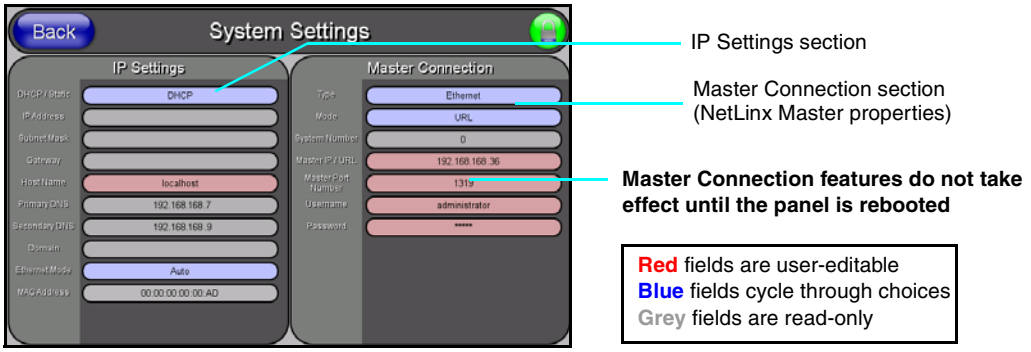


FIG. 114 System Settings page showing default values (reads and assigns values to the panel and Master)

The elements of the System Settings page are described in the table below:

System Settings Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).

System Settings Page Elements (Cont.)	
IP Settings:	Sets the IP communication values for the panel and contains:
DHCP/Static	Sets the panel to either DHCP or Static communication modes. • *DHCP (Dynamic Host Configuration Protocol)* assigns IP Addresses from client stations logging onto a TCP/IP network via a DHCP server. • *Static IP* is a permanent IP Address that is assigned to a node in a TCP/IP network.
IP Address	Sets the secondary IP Address assigned to the panel.
Subnet Mask	Sets a subnetwork address to the panel. • *Subnetwork mask* is the technique used by the IP protocol to filter messages into a particular network segment (Subnet).
Gateway	Sets a gateway value to the panel. • *Gateway* is a computer that either performs protocol conversion between different types of networks/applications or acts as a go-between two or more networks that use the same protocols.
Host Name	Sets the host name of the panel.
Primary DNS	Sets the address of the primary DNS server used for host name lookups. • *DNS (Domain Name System)* is software that lets users locate computers on a local network or the Internet (TCP/IP network) by host and domain. The DNS server maintains a database of host names for its' domain and their corresponding IP Addresses.
Secondary DNS	Sets a secondary DNS value to the panel.
Domain	Sets the unique name on the Internet to the panel for DNS look-up. • The panel belongs to the DNS domain.
Ethernet Mode	Sets the speed of the Ethernet connection to the panel. • Choices are: **Auto**, **10 Half Duplex**, **10 Full Duplex**, **100 Half Duplex,** or **100 Full Duplex.**
MAC Address	Displays a read-only field that is factory set by AMX for the built-in Ethernet interface.
Master Connection:	Sets the NetLinx Master communication values:
Type	Sets the NetLinx Master to communicate with the panel via either USB or Ethernet. This is based on the cable connection from the rear. ***ICSNet is not a supported option on this panel.*** • *Ethernet* is a CAT-5 cable (10/100Base T terminated in an RJ-45 connector) used to network computers together and is used in most LAN (local area networks). This description is also used to refer to both wired and wireless communication. • *USB* option cannot be used on Modero panels which are not equipped with a rear USB port.
Mode	Cycles between the different connection modes (URL, Listen, and Auto) ***(ETHERNET Only - disabled when USB is selected)*** • **URL** - In this mode, enter the IP/URL, Master Port Number, and username/password (if used) on the Master. - The System Number field is read-only because the panel obtains this information from the communicating Master. • **Listen** - In this mode, add the Modero panel address into the URL List in NetLinx Studio and set the connection mode to Listen. This mode allows the Modero touch panel to "listen" for the Master's communication signals. - The System Number and Master IP/URL fields are red-only. • **Auto** - In this mode, enter the System Number and a username/password (if applicable). This mode is used when both the panel and the NetLinx Master are on the same Subnet and the Master has its UDP feature enabled. - Master IP/URL field is read-only.

System Settings Page Elements (Cont.)	
Master Connection (Cont.):	
System Number	Allows you to enter a system number. Default value is 0 (zero). ***(ETHERNET Only - disabled when USB is selected)***
Master IP/URL	Sets the Master IP or URL of the NetLinx Master. ***(ETHERNET Only - disabled when USB is selected)***
Master Port Number	Allows you to enter the port number used with the NetLinx Master. • Default value is 1319. ***(ETHERNET Only - disabled when USB is selected)***
Username/Password	If the target Master has been previously secured, enter the alpha-numeric string (into each field) assigned to a pre-configured user profile on the Master. This profile should have the pre-defined level of access/configuration rights.

Refer to the *Step 2: Choose a Master Connection Mode Setting* section on page 71 for more detailed information on using the System Settings page.

Programming

You can program the touch panel, using the commands in this section, to perform a wide variety of operations using Send_Commands and variable text commands.

A device must first be defined in the NetLinx programming language with values for the Device: Port: System (in all programming examples - ***Panel*** is used in place of these values and represents all Modero panels).

Verify you are using the latest NetLinx Master and Modero firmware.
Verify you are using the latest version of NetLinx Studio and TPD4.

Button Assignments

- Button Channel Range: 1 - 4000 Button push and Feedback (per address port)
- Button Variable Text range: 1 - 4000 (per address port)
- Button States Range: 1 - 256
  (0 = All states, for General buttons 1 = Off state and 2 = On state).
- Level Range: 1 - 600 (Default level value 0 - 255, can be set up to 1 - 65535)
- Address port Range: 1 - 100

These button assignments can only be adjusted in TPD4 and not on the panels themselves.

Page Commands

These Page Commands are used in NetLinx Programming Language and are case insensitive.

Page Commands	

@APG
Add a specific popup page to a specified popup group.
	Add the popup page to a group if it does not already exist. If the new popup is added to a group which has a popup displayed on the current page along with the new pop-up, the displayed popup will be hidden and the new popup will be displayed.
	Syntax:
	`"'@APG-<popup page name>;<popup group name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	popup group name = 1 - 50 ASCII characters. Name of the popup group.
	Example:
	`SEND_COMMAND Panel,"'@APG-Popup1;Group1'"`
	Adds the popup page 'Popup1' to the popup group 'Group1'.

@CPG
Clear all popup pages from specified popup group.
	Syntax:
	`"'@CPG-<popup group name>'"`
	Variable:
	popup group name = 1 - 50 ASCII characters. Name of the popup group.
	Example:
	`SEND_COMMAND Panel,"'@CPG-Group1'"`
	Clears all popup pages from the popup group 'Group1'.

Page Commands (Cont.)	

@DPG
Delete a specific popup page from specified popup group if it exists.
	Syntax:
	`"'@DPG-<popup page name>;<popup group name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	popup group name = 1 - 50 ASCII characters. Name of the popup group.
	Example:
	`SEND_COMMAND Panel,"'@DPG-Popup1;Group1'"`
	Deletes the popup page 'Popup1' from the popup group 'Group1'.

@PDR
Set the popup location reset flag.
	If the flag is set, the popup will return to its default location on show instead of its last drag location.
	Syntax:
	`"'@PDR-<popup page name>;<reset flag>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	reset flag = 1 = Enable reset flag
	0 = Disable reset flag
	Example:
	`SEND_COMMAND Panel,"'@PDR-Popup1;1'"`
	Popup1 will return to its default location when turned On.

@PHE
Set the hide effect for the specified popup page to the named hide effect.
	Syntax:
	`"'@PHE-<popup page name>;<hide effect name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	hide effect name = Refers to the popup effect names being used.
	Example:
	`SEND_COMMAND Panel,"'@PHE-Popup1;Slide to Left'"`
	Sets the Popup1 hide effect name to 'Slide to Left'.

@PHP
Set the hide effect position.
	Only 1 coordinate is ever needed for an effect; however, the command will specify both. This command sets the location at which the effect will end at.
	Syntax:
	`"'@PHP-<popup page name>;<x coordinate>,<y coordinate>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PHP-Popup1;75,0'"`
	Sets the Popup1 hide effect x-coordinate value to 75 and the y-coordinate value to 0.

@PHT
Set the hide effect time for the specified popup page.
	Syntax:
	`"'@PHT-<popup page name>;<hide effect time>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	hide effect time = Given in 1/10ths of a second.
	Example:
	`SEND_COMMAND Panel,"'@PHT-Popup1;50'"`
	Sets the Popup1 hide effect time to 5 seconds.

Page Commands (Cont.)	

@PPA
Close all popups on a specified page.
	If the page name is empty, the current page is used. Same as the 'Clear Page' command in TPDesign4.
	Syntax:
	`"'@PPA-<page name>'"`
	Variable:
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPA-Page1'"`
	Close all popups on Page1.

@PPF
Deactivate a specific popup page on either a specified page or the current page.
	If the page name is empty, the current page is used (see example 2). If the popup page is part of a group, the whole group is deactivated. This command works in the same way as the 'Hide Popup' command in TPDesign4.
	Syntax:
	`"'@PPF-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPF-Popup1;Main'"`
	Deactivates the popup page 'Popup1' on the Main page.
	Example 2:
	`SEND_COMMAND Panel,"'@PPF-Popup1'"`
	Deactivates the popup page 'Popup1' on the current page.

@PPG
Toggle a specific popup page on either a specified page or the current page.
	If the page name is empty, the current page is used (see example 2). Toggling refers to the activating/deactivating (On/Off) of a popup page. This command works in the same way as the 'Toggle Popup' command in TPDesign4.
	Syntax:
	`"'@PPG-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPG-Popup1;Main'"`
	Toggles the popup page 'Popup1' on the 'Main' page from one state to another (On/Off).
	Example 2:
	`SEND_COMMAND Panel,"'@PPG-Popup1'"`
	Toggles the popup page 'Popup1' on the current page from one state to another (On/Off).

@PPK
Kill a specific popup page from all pages.
	Kill refers to the deactivating (Off) of a popup window from all pages. If the pop-up page is part of a group, the whole group is deactivated. This command works in the same way as the 'Clear Group' command in TPDesign 4.
	Syntax:
	`"'@PPK-<popup page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	Example:
	`SEND_COMMAND Panel,"'@PPK-Popup1'"`
	Kills the popup page 'Popup1' on all pages.

Page Commands (Cont.)	

@PPM
Set the modality of a specific popup page to Modal or NonModal.
	A Modal popup page, when active, only allows you to use the buttons and features on that popup page. All other buttons on the panel page are inactivated.
	Syntax:
	`"'@PPM-<popup page name>;<mode>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	mode = NONMODAL converts a previously Modal popup page to a NonModal.
	MODAL converts a previously NonModal popup page to Modal.
	modal = 1 and non-modal = 0
	Example:
	`SEND_COMMAND Panel,"'@PPM-Popup1;Modal'"`
	Sets the popup page 'Popup1' to Modal.
	`SEND_COMMAND Panel,"'@PPM-Popup1;1'"`
	Sets the popup page 'Popup1' to Modal.

@PPN
Activate a specific popup page to launch on either a specified page or the current page.
	If the page name is empty, the current page is used (see example 2). If the popup page is already on, do not re-draw it. This command works in the same way as the 'Show Popup' command in TPDesign4.
	Syntax:
	`"'@PPN-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPN-Popup1;Main'"`
	Activates 'Popup1' on the 'Main' page.
	Example 2:
	`SEND_COMMAND Panel,"'@PPN-Popup1'"`
	Activates the popup page 'Popup1' on the current page.

@PPT
Set a specific popup page to timeout within a specified time.
	If timeout is empty, popup page will clear the timeout.
	Syntax:
	`"'@PPT-<popup page name>;<timeout>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	timeout = Timeout duration in 1/10ths of a second.
	Example:
	`SEND_COMMAND Panel,"'@PPT-Popup1;30'"`
	Sets the popup page 'Popup1' to timeout within 3 seconds.

@PPX
Close all popups on all pages.
	This command works in the same way as the 'Clear All' command in TPDesign 4.
	Syntax:
	`"'@PPX'"`
	Example:
	`SEND_COMMAND Panel,"'@PPX'"`
	Close all popups on all pages.

Page Commands (Cont.)	

@PSE
Set the show effect for the specified popup page to the named show effect.
	Syntax:
	`"'@PSE-<popup page name>;<show effect name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	show effect name = Refers to the popup effect name being used.
	Example:
	`SEND_COMMAND Panel,"'@PSE-Popup1;Slide from Left'"`
	Sets the Popup1 show effect name to 'Slide from Left'.

@PSP
Set the show effect position.
	Only 1 coordinate is ever needed for an effect; however, the command will specify both. This command sets the location at which the effect will begin at.
	Syntax:
	`"'@PSP-<popup page name>;<x coordinate>,<y coordinate>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PSP-Popup1;100,0'"`
	Sets the Popup1 show effect x-coordinate value to 100 and the y-coordinate value to 0.

@PST
Set the show effect time for the specified popup page.
	Syntax:
	`"'@PST-<popup page name>;<show effect time>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	show effect time = Given in 1/10ths of a second.
	Example:
	`SEND_COMMAND Panel,"'@PST-Popup1;50'"`
	Sets the Popup1 show effect time to 5 seconds.

PAGE
Flip to a specified page.
	Flips to a page with a specified page name. If the page is currently active, it will not redraw the page.
	Syntax:
	`"'PAGE-<page name>'"`
	Variable:
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PAGE-Page1'"`
	Flips to page1.

Page Commands (Cont.)	

PPOF
Deactivate a specific popup page on either a specified page or the current page.
	If the page name is empty, the current page is used (see example 2). If the popup page is part of a group, the whole group is deactivated. This command works in the same way as the 'Hide Popup' command in TPDesign4.
	Syntax:
	`"'PPOF-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PPOF-Popup1;Main'"`
	Deactivates the popup page 'Popup1' on the Main page.
	Example 2:
	`SEND_COMMAND Panel,"'PPOF-Popup1'"`
	Deactivates the popup page 'Popup1' on the current page.

PPOG
Toggle a specific popup page on either a specified page or the current page.
	If the page name is empty, the current page is used (see example 2). Toggling refers to the activating/deactivating (On/Off) of a popup page. This command works in the same way as the 'Toggle Popup' command in TPDesign4.
	Syntax:
	`"'PPOG-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PPOG-Popup1;Main'"`
	Toggles the popup page 'Popup1' on the Main page from one state to another (On/Off).
	Example 2:
	`SEND_COMMAND Panel,"'PPOG-Popup1'"`
	Toggles the popup page 'Popup1' on the current page from one state to another (On/Off).

PPON
Activate a specific popup page to launch on either a specified page or the current page.
	If the page name is empty, the current page is used (see example 2). If the popup page is already On, do not re-draw it. This command works in the same way as the 'Show Popup' command in TPDesign4.
	Syntax:
	`"'PPON-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PPON-Popup1; Main'"`
	Activates the popup page 'Popup1' on the Main page.
	Example 2:
	`SEND_COMMAND Panel,"'PPON-Popup1'"`
	Activates the popup page 'Popup1' on the current page.

Programming Numbers

The following information provides the programming numbers for colors, fonts, and borders.

Colors can be used to set the colors on buttons, sliders, and pages. The lowest color number represents the lightest color-specific display; the highest number represents the darkest display. For example, 0 represents light red, and 5 is dark red.

RGB triplets and names for basic 88 colors

RGB Values for all 88 Basic Colors				
Index No.	Name	Red	Green	Blue
00	Very Light Red	255	0	0
01	Light Red	223	0	0
02	Red	191	0	0
03	Medium Red	159	0	0
04	Dark Red	127	0	0
05	Very Dark Red	95	0	0
06	Very Light Orange	255	128	0
07	Light Orange	223	112	0
08	Orange	191	96	0
09	Medium Orange	159	80	0
10	Dark Orange	127	64	0
11	Very Dark Orange	95	48	0
12	Very Light Yellow	255	255	0
13	Light Yellow	223	223	0
14	Yellow	191	191	0
15	Medium Yellow	159	159	0
16	Dark Yellow	127	127	0
17	Very Dark Yellow	95	95	0
18	Very Light Lime	128	255	0
19	Light Lime	112	223	0
20	Lime	96	191	0
21	Medium Lime	80	159	0
22	Dark Lime	64	127	0
23	Very Dark Lime	48	95	0
24	Very Light Green	0	255	0
25	Light Green	0	223	0
26	Green	0	191	0
27	Medium Green	0	159	0
28	Dark Green	0	127	0
29	Very Dark Green	0	95	0
30	Very Light Mint	0	255	128
31	Light Mint	0	223	112
32	Mint	0	191	96
33	Medium Mint	0	159	80
34	Dark Mint	0	127	64
35	Very Dark Mint	0	95	48

RGB Values for all 88 Basic Colors (Cont.)				
Index No.	Name	Red	Green	Blue
36	Very Light Cyan	0	255	255
37	Light Cyan	0	223	223
38	Cyan	0	191	191
39	Medium Cyan	0	159	159
40	Dark Cyan	0	127	127
41	Very Dark Cyan	0	95	95
42	Very Light Aqua	0	128	255
43	Light Aqua	0	112	223
44	Aqua	0	96	191
45	Medium Aqua	0	80	159
46	Dark Aqua	0	64	127
47	Very Dark Aqua	0	48	95
48	Very Light Blue	0	0	255
49	Light Blue	0	0	223
50	Blue	0	0	191
51	Medium Blue	0	0	159
52	Dark Blue	0	0	127
53	Very Dark Blue	0	0	95
54	Very Light Purple	128	0	255
55	Light Purple	112	0	223
56	Purple	96	0	191
57	Medium Purple	80	0	159
58	Dark Purple	64	0	127
59	Very Dark Purple	48	0	95
60	Very Light Magenta	255	0	255
61	Light Magenta	223	0	223
62	Magenta	191	0	191
63	Medium Magenta	159	0	159
64	Dark Magenta	127	0	127
65	Very Dark Magenta	95	0	95
66	Very Light Pink	255	0	128
67	Light Pink	223	0	112
68	Pink	191	0	96
69	Medium Pink	159	0	80
70	Dark Pink	127	0	64
71	Very Dark Pink	95	0	48
72	White	255	255	255
73	Grey1	238	238	238
74	Grey3	204	204	204
75	Grey5	170	170	170
76	Grey7	136	136	136
77	Grey9	102	102	102
78	Grey4	187	187	187
79	Grey6	153	153	153

RGB Values for all 88 Basic Colors (Cont.)				
Index No.	Name	Red	Green	Blue
80	Grey8	119	119	119
81	Grey10	85	85	85
82	Grey12	51	51	51
83	Grey13	34	34	34
84	Grey2	221	221	221
85	Grey11	68	68	68
86	Grey14	17	17	17
87	Black	0	0	0
255	TRANSPARENT	99	53	99

Font styles and ID numbers

Font styles can be used to program the text fonts on buttons, sliders, and pages. The following chart shows the default font type and their respective ID numbers generated by TPDesign4.

Default Font Styles and ID Numbers						
Font ID #	Font type	Size		Font ID #	Font type	Size
1	Courier New	9		19	Arial	9
2	Courier New	12		20	Arial	10
3	Courier New	18		21	Arial	12
4	Courier New	26		22	Arial	14
5	Courier New	32		23	Arial	16
6	Courier New	18		24	Arial	18
7	Courier New	26		25	Arial	20
8	Courier New	34		26	Arial	24
9	AMX Bold	14		27	Arial	36
10	AMX Bold	20		28	Arial Bold	10
11	AMX Bold	36		29	Arial Bold	8
				32 - Variable Fonts start at 32.		

NOTE

You must import fonts into a TPDesign4 project file. The font ID numbers are assigned by TPDesign4. These values are also listed in the ***Generate Programmer's Report****.*

Border styles

The TPDesign4 Touch Panel Design program has pre-set border styles that are user selectable. TPD4 border styles can ONLY be changed by using the name.

TPD4 Border Styles by Name	
Border styles	Border styles
None	Diamond 55
AMX Elite -L	Diamond 65
AMX Elite -M	Diamond 75
AMX Elite -S	Double Bevel -L
Bevel -L	Double Bevel -M
Bevel -M	Double Bevel -S
Bevel -S	Double Line
Circle 15	Fuzzy
Circle 25	Glow-L
Circle 35	Help Down
Circle 45	Help Down Reversed
Circle 55	Menu Bottom Rounded 15
Circle 65	Menu Bottom Rounded 25
Circle 75	Menu Bottom Rounded 35
Circle 85	Menu Bottom Rounded 45
Circle 95	Menu Bottom Rounded 55
Circle 105	Menu Bottom Rounded 65
Circle 115	Menu Bottom Rounded 75
Circle 125	Menu Bottom Rounded 85
Circle 135	Menu Bottom Rounded 95
Circle 145	Menu Bottom Rounded 105
Circle 155	Menu Bottom Rounded 115
Circle 165	Menu Bottom Rounded 125
Circle 175	Menu Bottom Rounded 135
Circle 185	Menu Bottom Rounded 145
Circle 195	Menu Bottom Rounded 155
Cursor Bottom	Menu Bottom Rounded 165
Cursor Bottom with Hole	Menu Bottom Rounded 175
Cursor Top	Menu Bottom Rounded 185
Cursor Top with Hole	Menu Bottom Rounded 195
Cursor Left	Menu Left Rounded 15
Cursor Left with Hole	Menu Left Rounded 25
Cursor Right	Menu Left Rounded 35
Cursor Right with Hole	Menu Left Rounded 45
Custom Frame	Menu Left Rounded 55
Diamond 15	Menu Left Rounded 65
Diamond 25	Menu Left Rounded 75
Diamond 35	Menu Left Rounded 85
Diamond 45	Menu Left Rounded 95

TPD4 Border Styles by Name (Cont.)	
Border styles	Border styles
Menu Left Rounded 105	Menu Top Rounded 65
Menu Left Rounded 115	Menu Top Rounded 75
Menu Left Rounded 125	Menu Top Rounded 85
Menu Left Rounded 135	Menu Top Rounded 95
Menu Left Rounded 145	Menu Top Rounded 105
Menu Left Rounded 155	Menu Top Rounded 115
Menu Left Rounded 165	Menu Top Rounded 125
Menu Left Rounded 175	Menu Top Rounded 135
Menu Left Rounded 185	Menu Top Rounded 145
Menu Left Rounded 195	Menu Top Rounded 155
Menu Right Rounded 15	Menu Top Rounded 165
Menu Right Rounded 25	Menu Top Rounded 175
Menu Right Rounded 35	Menu Top Rounded 185
Menu Right Rounded 45	Menu Top Rounded 195
Menu Right Rounded 55	Neon Active -L
Menu Right Rounded 65	Neon Active -S
Menu Right Rounded 75	Neon Inactive -L
Menu Right Rounded 85	Neon Inactive -S
Menu Right Rounded 95	Oval V 30x60
Menu Right Rounded 105	Oval V 50x100
Menu Right Rounded 115	Oval V 75x150
Menu Right Rounded 125	Oval V 100x200
Menu Right Rounded 135	Oval H 60x30
Menu Right Rounded 145	Oval H 100x50
Menu Right Rounded 155	Oval H 150x75
Menu Right Rounded 165	Oval H 200x100
Menu Right Rounded 175	Picture Frame
Menu Right Rounded 185	Quad Line
Menu Right Rounded 195	Single Line
Menu Rounded Spacer - Vertical	Windows Style Popup
Menu Rounded Spacer - Horizontal	Window Style Popup (Status Bar)
Menu Top Rounded 55	

"^" Button Commands

These Button Commands are used in NetLinx Studio and are case insensitive.

All commands that begin with "^" have the capability of assigning a variable text address range and button state range. **A device must first be defined in the NetLinx programming language with values for the Device: Port : System** (in all programming examples - ***Panel*** is used in place of these values).

- **Variable text ranges** allow you to target 1 or more variable text channels in a single command.
- **Button State ranges** allow you to target 1 or more states of a variable text button with a single command.
- **"."** Character is used for the 'through' notation, also the "**&**" character is used for the 'And' notation.

"^" Button Commands	

^ANI
Run a button animation (in 1/10 second).
	Syntax:
	`"'^ANI-<vt addr range>,<start state>,<end state>,<time>'"`
	Variable:
	variable text address range = 1 - 4000.
	start state = Beginning of button state (0= current state).
	end state = End of button state.
	time = In 1/10 second intervals.
	Example:
	`SEND_COMMAND Panel,"'^ANI-500,1,25,100'"`
	Runs a button animation at text range 500 from state 1 to state 25 for 10 second.

^APF
Add page flip action to a button if it does not already exist.
	Syntax:
	`"'^APF-<vt addr range>,<page flip action>,<page name>'"`
	Variable:
	variable text address range = 1 - 4000.
	page flip action = **Stan**[dardPage] - Flip to standard page
	Prev[iousPage] - Flip to previous page
	Show[Popup] - Show Popup page
	Hide[Popup] - Hide Popup page
	Togg[lePopup] - Toggle popup state
	ClearG[roup] - Clear popup page group from all pages
	ClearP[age] - Clear all popup pages from a page with the specified page name
	ClearA[ll] - Clear all popup pages from all pages
	page name = 1 - 50 ASCII characters.
	Example:
	`SEND COMMAND Panel,"'^APF-400,Stan,Main Page'"`
	Assigns a button to a standard page flip with page name 'Main Page'.

"^" Button Commands (Cont.)	

^BAT
Append non-unicode text.
	Syntax:
	`"'^BAT-<vt addr range>,<button states range>,<new text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^BAT-520,1,Enter City'"`
	Appends the text 'Enter City' to the button's OFF state.

^BAU
Append unicode text.
	Same format as ^UNI.
	Syntax:
	`"'^BAU-<vt addr range>,<button states range>,<unicode text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	unicode text = 1 - 50 ASCII characters. Unicode characters must be entered in Hex format.
	Example:
	`SEND_COMMAND Panel,"'^BAU-520,1,00770062'"`
	Appends Unicode text '00770062' to the button's OFF state.

"^" Button Commands (Cont.)	

^BCB
Set the border color to the specified color.
	Only if the specified border color is not the same as the current color.
	Note: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).
	Syntax:
	`"'^BCB-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to theRGB Values for all 88 Basic Colors table on page 141 for more information.
	Example:
	`SEND_COMMAND Panel,"'^BCB-500.504&510,1,12'"`
	Sets the Off state border color to 12 (Yellow). Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB). Refer to theRGB Values for all 88 Basic Colors table on page 141.

^BCF
Set the fill color to the specified color.
	Only if the specified fill color is not the same as the current color.
	Note: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).
	Syntax:
	`"'^BCF-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to theRGB Values for all 88 Basic Colors table on page 141 for more information.
	Example:
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,12'"`
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,Yellow'"`
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A63''"`
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A'"`
	Sets the Off state fill color by color number. Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB).

"^" Button Commands (Cont.)	

^BCT
Set the text color to the specified color.
	Only if the specified text color is not the same as the current color.
	Note: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).
	Syntax:
	`"'^BCT-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to theRGB Values for all 88 Basic Colors table on page 141 for more information.
	Example:
	`SEND_COMMAND Panel,"'^BCT-500.504&510,1,12'"`
	Sets the Off state border color to 12 (Yellow). Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB).

^BDO
Set the button draw order.
	Determines what order each layer of the button is drawn.
	Syntax:
	`"'^BDO-<vt addr range>,<button states range>,<1-5><1-5><1-5><1-5><1-5>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	layer assignments = Fill Layer = 1
	Image Layer = 2
	Icon Layer = 3
	Text Layer = 4
	Border Layer = 5
	***Note**: The layer assignments are from bottom to top. The default draw order is* **12345**.
	Example:
	`SEND_COMMAND Panel,"'^BDO-530,1&2,51432'"`
	Sets the button's variable text 530 ON/OFF state draw order (from bottom to top) to Border, Fill, Text, Icon, and Image.
	Example 2:
	`SEND_COMMAND Panel,"'^BDO-1,0,12345'"`
	Sets all states of a button back to its default drawing order.

^BFB
Set the feedback type of the button.
	ONLY works on General-type buttons.
	Syntax:
	`"'^BFB-<vt addr range>,<feedback type>'"`
	Variable:
	variable text address range = 1 - 4000.
	feedback type = (None, Channel, Invert, On (Always on), Momentary, and Blink).
	Example:
	`SEND_COMMAND Panel,"'^BFB-500,Momentary'"`
	Sets the Feedback type of the button to 'Momentary'.

"^" Button Commands (Cont.)	

^BIM
Set the input mask for the specified address.
	Syntax:
	`"'^BIM-<vt addr range>,<input mask>'"`
	Variable:
	variable text address range = 1 - 4000.
	input mask = Refer to the *Text Area Input Masking* section on page 192 for character types.
	Example:
	`SEND_COMMAND Panel,"'^BIM-500,AAAAAAAAAA'"`
	Sets the input mask to ten 'A' characters, that are required, to either a letter or digit **(entry is required).**

^BLN
Set the number of lines removed equally from the top and bottom of a composite video signal.
	The maximum number of lines to remove is 240. A value of 0 will display the incoming video signal unaffected. This command is used to scale non 4x3 video images into non 4x3 video buttons.
	Syntax:
	`"'^BLN-<vt addr range>,<button states range>,<number of lines>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	number of lines = 0 - 240.
	Example:
	`SEND_COMMAND Panel,"'^BLN-500,55'"`
	Equally removes 55 lines from the top and 55 lines from the bottom of the video button.

"^" Button Commands (Cont.)	

^BMC
Button copy command. Copy attributes of the source button to all the destination buttons.
	Note that the source is a single button state. Each state must be copied as a separate command. The <codes> section represents what attributes will be copied. All codes are 2 char pairs that can be separated by comma, space, percent or just ran together.
	Syntax:
	`"'^BMC-<vt addr range>,<button states range>,<source port>,<source address>,<source state>,<codes>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	source port = 1 - 100.
	source address = 1 - 4000.
	source state = 1 - 256.
	codes: BM - Picture/Bitmap
	BR - Border
	CB - Border Color
	CF - Fill Color
	CT - Text Color
	EC - Text effect color
	EF - Text effect
	FT - Font
	IC - Icon
	JB - Bitmap alignment
	JI - Icon alignment
	JT - Text alignment
	LN - Lines of video removed
	OP - Opacity
	SO - Button Sound
	TX - Text
	VI - Video slot ID
	WW - Word wrap on/off
	Example:
	`SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,BR'"`
	`or`
	`SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,%BR'"`
	Copies the OFF state border of button with a variable text address of 500 onto the OFF state border of button with a variable text address of 425.
	Example 2:
	`SEND_COMMAND Panel,"'^BMC-150,1,1,315,1,%BR%FT%TX%BM%IC%CF%CT'"`
	Copies the OFF state border, font, Text, bitmap, icon, fill color and text color of the button with a variable text address of 315 onto the OFF state border, font, Text, bitmap, icon, fill color and text color of the button with a variable text address of 150.

"^" Button Commands (Cont.)	
^BMF Set any/all button parameters by sending embedded codes and data.	Syntax: "'^BMF-<vt addr range>,<button states range>,<data>'" Variables: variable text address char array = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). level range = 1 - 600 (level value is 1 - 65535). data: '%B<border style>' = Set the border style name. See theTPD4 Border Styles by Name table on page 144. '%B',<border 0-27,40,41> = Set the borer style number. See theTPD4 Border Styles by Name table on page 144. '%DO<1-5><1-5><1-5><1-5><1-5> = Set the draw order. Listed from bottom to top. Refer to the ^BDO command on page 149 for more information. '%F',<font 1-8,10,11,20-29,32-xx> = Set the font. See theDefault Font Styles and ID Numbers table on page 143. '%F<font 01-08,10,11,20-29,32-xx>' = Set the font. See theDefault Font Styles and ID Numbers table on page 143. '%MI<mask image>' = Set the mask image. Refer to the ^BMI command on page 154 for more information. '%T<text >' = Set the text using ASCII characters (empty is clear). '%P<bitmap>' = Set the picture/bitmap filename (empty is clear). '%I',<icon 01-9900, 0-clear>' = Set the icon using values of 01 - 9900 (icon numbers are assigned in the TPDesign4 Resource Manager tab - Slots section). '%I<icon 01-9900, 0-clear>' = Set the icon using values of 01 - 9900 (icon numbers are assigned in the TPDesign4 Resource Manager tab - Slots section). '%J',<alignment of text 1-9> = As shown the following telephone keypad alignment chart: 0 1 2 3 4 5 6 7 8 9 Zero can be used for an absolute position '%JT<alignment of text 0-9>' = As shown the above telephone keypad alignment chart, **BUT** the 0 (zero) is absolute and followed by **',<left>,<top>'** '%JB<alignment of bitmap/picture 0-9>' = As shown the above telephone keypad alignment chart BUT the 0 (zero) is absolute and followed by **',<left>,<top>'** '%JI<alignment of icon 0-9>' = As shown the above telephone keypad alignment chart, **BUT** the 0 (zero) is absolute and followed by **',<left>,<top>'**

"^" Button Commands (Cont.)	
^BMF (Cont.)	*For some of these commands and values, refer to* theRGB Values for all 88 Basic Colors table on page 141. '%CF<on fill color>' = Set Fill Color. '%CB<on border color>' = Set Border Color. '%CT<on text color>' = Set Text Color. '%SW<1 or 0>' = Show/hide a button. '%ST<style>' = Button style. '%SO<sound>' = Set the button sound. '%EN<1 or 0>' = Enable/disable a button. '%WW<1 or 0>' = Word wrap On/Off. '%GH<bargraph hi>' = Set the bargraph upper limit. '%GL<bargraph low>' = Set the bargraph lower limit. '%GN<bargraph slider name>' = Set the bargraph slider name/Joystick cursor name. '%GC<bargraph slider color>' = Set the bargraph slider color/Joystick cursor color. '%GI<bargraph invert>' = Set the bargraph invert/noninvert or joystick coordinate (0,1,2,3). See the ^GIV command on page 160 for more information. '%GU<bargraph ramp up>' = Set the bargraph ramp up time in intervals of 1/10 second. '%GD<bargraph ramp down>' = Set the bargraph ramp down time in 1/10 second. '%GG<bargraph drag increment> = Set the bargraph drag increment. Refer to the ^GDI command on page 160 for more information. '%VI<video ON/OFF>' = Set the Video either ON (value=1) or OFF (value=0). '%OT<feedback type>' = Set the Feedback (Output) Type to one of the following: None, Channel,Invert, ON (Always ON), Momentary, or Blink. '%SM' = Submit a text for text area button. '%SF<1 or 0>' = Set the focus for text area button. '%OP<0-255>' = Set the button opacity to either Invisible (value=0) or Opaque (value=255). '%OP#<00-FF>' = Set the button opacity to either Invisible (value=00) or Opaque (value=FF). '%UN<Unicode text>' = Set the Unicode text. See the*^UNI* section on page 165 for the text format. '%LN<0-240>' = Set the lines of video being removed. See the*^BLN* section on page 150 for more information. '%EF<text effect name>' = Set the text effect. '%EC<text effect color>' = Set the text effect color. '%ML<max length>' = Set the maximum length of a text area. '%MK<input mask>' = Set the input mask of a text area. '%VL<0-1>' = Log-On/Log-Off the computer control connection '%VN<network name>' = Set network connection name. '%VP<password>' = Set the network connection password. Example: `SEND_COMMAND Panel,"'^BMF-500,1,%B10%CFRed%CB Blue %CTBlack%Ptest.png'"` Sets the button OFF state as well as the Border, Fill Color, Border Color, Text Color, and Bitmap.

"^" Button Commands (Cont.)	

^BMI
Set the button mask image.
	Mask image is used to crop a borderless button to a non-square shape. This is typically used with a bitmap.
	Syntax:
	`"'^BMI-<vt addr range>,<button states range>,<mask image>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	mask image = Graphic file used.
	Example:
	`SEND_COMMAND Panel,"'^BMI-530,1&2,newMac.png'"`
	Sets the button with variable text 530 ON/OFF state mask image to 'newmac.png'.

^BML
Set the maximum length of the text area button.
	If this value is set to zero (0) there is no max length. The maximum length available is 2000. This is only for a Text area input button and not for a Text area input masking button.
	Syntax:
	`"'^BML-<vt addr range>,<max length>'"`
	Variable:
	variable text address range = 1 - 4000.
	max length = 2000 (0=no max length).
	Example:
	`SEND_COMMAND Panel,"'^BML-500,20'"`
	Sets the maximum length of the text area input button to 20 characters.

^BMP
Assign a picture to those buttons with a defined address range.
	Syntax:
	`"'^BMP-<vt addr range>,<button states range>,<name of bitmap/ picture>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	name of bitmap/picture = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^BMP-500.504&510.515,1,bitmap.png'"`
	Sets the OFF state picture for the buttons with variable text ranges of 500-504 & 510-515.

^BNC
Clear current TakeNote annotations.
	Syntax:
	`"'^BNC-<vt addr range>,<command value>'"`
	Variable:
	variable text address range = 1 - 4000.
	command value = (0= clear, 1= clear all).
	Example:
	`SEND_COMMAND Panel,"'^BNC-973,0'"`
	Clears the annotation of the TakeNote button with variable text 973.

"^" Button Commands (Cont.)	

^BNN
Set the TakeNote network name for the specified Addresses.
	Syntax:
	`"'^BNN-<vt addr range>,<network name>'"`
	Variable:
	variable text address range = 1 - 4000.
	network name = Use a valid IP Address.
	Example:
	`SEND_COMMAND Panel,"'^BNN-973,192.168.169.99'"`
	Sets the TakeNote button network name to 192.168.169.99.

^BNT
Set the TakeNote network port for the specified Addresses.
	Syntax:
	`"'^BNT-<vt addr range>,<network port>'"`
	Variable:
	variable text address range = 1 - 4000.
	network port = 1 - 65535.
	Example:
	`SEND_COMMAND Panel,"'^BNT-973,5000'"`
	Sets the TakeNote button network port to 5000.

^BOP
Set the button opacity.
	The button opacity can be specified as a decimal between 0 - 255, where zero (0) is invisible and 255 is opaque, or as a HEX code, as used in the color commands by preceding the HEX code with the # sign. In this case, #00 becomes invisible and #FF becomes opaque. If the opacity is set to zero (0), this does not make the button inactive, only invisible.
	Syntax:
	`"'^BOP-<vt addr range>,<button states range>,<button opacity>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	button opacity = 0 (invisible) - 255 (opaque).
	Example:
	`SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,200'"`
	Example 2:
	`SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,#C8'"`
	Both examples set the opacity of the buttons with the variable text range of 500-504 and 510-515 to 200.

"^" Button Commands (Cont.)	

^BOR
Set a border to a specific border style associated with a border value for those buttons with a defined address range.
	Refer to theTPD4 Border Styles by Name table on page 144 for more information.
	Syntax:
	`"'^BOR-<vt addr range>,<border style name or border value>'"`
	Variable:
	variable text address range = 1 - 4000.
	border style name = Refer to the TPD4 Border Styles by Name table on page 144.
	border value = 0 - 41.
	Examples:
	`SEND_COMMAND Panel,"'^BOR-500.504&510.515,10'"`
	Sets the border by number (#10) to those buttons with the variable text range of 500-504 & 510-515.
	`SEND_COMMAND Panel,"'^BOR-500.504&510,AMX Elite -M'"`
	Sets the border by name (AMX Elite) to those buttons with the variable text range of 500-504 & 510-515.
	The border style is available through the TPDesign4 border-style drop-down list. Refer to theTPD4 Border Styles by Name table on page 144 for more information.

^BOS
Set the button to display either a Video or Non-Video window.
	Syntax:
	`"'^BOS-<vt addr range>,<button states range>,<video state>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	video state = Video Off = 0 and Video On = 1.
	Example:
	`SEND_COMMAND Panel,"'^BOS-500,1,1'"`
	Sets the button to display video.

^BPP
Set or clear the protected page flip flag of a button.
	Zero clears the flag.
	Syntax:
	`"'^BPP-<vt addr range>,<protected page flip flag value>'"`
	Variable:
	variable text address range = 1 - 4000.
	protected page flip flag value range = 0 - 4 (**0 clears the flag**).
	Example:
	`SEND_COMMAND Panel,"'^BPP-500,1'"`
	Sets the button to protected page flip flag 1 (sets it to password 1).

"^" Button Commands (Cont.)	

^BRD
Set the border of a button state/ states.
	Only if the specified border is not the same as the current border. The border names are available through the TPDesign4 border-name drop-down list.
	Syntax:
	`"'^BRD-<vt addr range>,<button states range>,<border name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	border name = Refer to TPD4 Border Styles by Name table on page 144.
	Example:
	`SEND_COMMAND Panel,"'^BRD-500.504&510.515,1&2,Quad Line'"`
	Sets the border by name (Quad Line) to those buttons with the variable text range of 500-504 & 510-515.
	Refer to the TPD4 Border Styles by Name table on page 144.

^BSF
Set the focus to the text area.
	Note: Select one button at a time (single variable text address). Do not assign a variable text address range to set focus to multiple buttons. Only one variable text address can be in focus at a time.
	Syntax:
	`"'^BSF-<vt addr range>,<selection value>'"`
	Variable:
	variable text address range = 1 - 4000.
	selection value = Unselect = 0 and select = 1.
	Example:
	`SEND_COMMAND Panel,"'^BSF-500,1'"`
	Sets the focus to the text area of the button.

^BSM
Submit text for text area buttons.
	This command causes the text areas to send their text as strings to the NetLinx Master.
	Syntax:
	`"'^BSM-<vt addr range>'"`
	Variable:
	variable text address range = 1 - 4000.
	Example:
	`SEND_COMMAND Panel,"'^BSM-500'"`
	Submits the text of the text area button.

^BSO
Set the sound played when a button is pressed.
	If the sound name is blank the sound is then cleared. If the sound name is not matched, the button sound is not changed.
	Syntax:
	`"'^BSO-<vt addr range>,<button states range>,<sound name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	sound name = (**blank** - sound cleared, **not matched** - button sound not changed).
	Example:
	`SEND_COMMAND Panel,"'^BSO-500,1&2,music.wav'"`
	Assigns the sound 'music.wav' to the button Off/On states.

"^" Button Commands (Cont.)	
^BVL Log-On/Log-Off the computer control connection.	Syntax: "'^BVL-<vt addr range>,<connection>'" Variable: variable text address range = 1 - 4000. connection = 0 (Log-Off connection) and 1 (Log-On connection). Example: SEND_COMMAND Panel,"'^BVL-500,0'" Logs-off the computer control connection of the button.
^BVN Set the computer control remote host for the specified address.	Syntax: SEND_COMMAND <DEV>,"'^BVN-<vt addr range>,<remote host>'" Variables: variable text address range = 1 - 4000. remote host = 1 - 50 ASCII characters. Example: SEND_COMMAND Panel,"'^BVN-500,191.191.191.191'" Sets the remote host to '191.191.191.191' for the specific computer control button.
^BVP Set the network password for the specified address.	Syntax: "'^BVP-<vt addr range>,<network password>'" Variable: variable text address range = 1 - 4000. network password = 1 - 50 ASCII characters. Example: SEND_COMMAND Panel,"'^BVP-500,PCLOCK'" Sets the password to PCLOCK for the specific PC control button.
^BVT Set the computer control network port for the specified address.	Syntax: "'^BVT-<vt addr range>,<network port>'" Variable: variable text address range = 1 - 4000. network port = 1 - 65535. Example: SEND_COMMAND Panel,"'^BVT-500,5000'" Sets the network port to 5000.
^BWW Set the button word wrap feature to those buttons with a defined address range.	By default, word-wrap is Off. Syntax: "'^BWW-<vt addr range>,<button states range>,<word wrap>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). word wrap = (0=Off and 1=On). Default is Off. Example: SEND_COMMAND Panel,"'^BWW-500,1,1'" Sets the word wrap on for the button's Off state.

"^" Button Commands (Cont.)	
^CPF Clear all page flips from a button.	Syntax: "'^CPF-<vt addr range>'" Variable: variable text address range = 1 - 4000. Example: SEND_COMMAND Panel,"'^CPF-500'" Clears all page flips from the button.
^DPF Delete page flips from button if it already exists.	Syntax: "'^DFP-<vt addr range>,<actions>,<page name>'" Variable: variable text address range = 1 - 4000. actions = **Stan**[dardPage] - Flip to standard page **Prev**[iousPage] - Flip to previous page **Show**[Popup] - Show Popup page **Hide**[Popup] - Hide Popup page **Togg**[lePopup] - Toggle popup state **ClearG**[roup] - Clear popup page group from all pages **ClearP**[age] - Clear all popup pages from a page with the specified page name **ClearA**[ll] - Clear all popup pages from all pages page name = 1 - 50 ASCII characters. Example: SEND COMMAND Panel,"'^DPF-409,Prev'" Deletes the assignment of a button from flipping to a previous page.
^ENA Enable or disable buttons with a set variable text range.	Syntax: "'^ENA-<vt addr range>,<command value>'" Variable: variable text address range = 1 - 4000. command value = (0= disable, 1= enable) Example: SEND_COMMAND Panel,"'^ENA-500.504&510.515,0'" Disables button pushes on buttons with variable text range 500-504 & 510-515.
^FON Set a font to a specific Font ID value for those buttons with a defined address range.	Font ID numbers are generated by the TPDesign4 programmers report. Syntax: "'^FON-<vt addr range>,<button states range>,<font value>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). font value = Range = 1 - XXX. Refer to theDefault Font Styles and ID Numbers table on page 143. Example: SEND_COMMAND Panel,"'^FON-500.504&510.515,1&2,4'" Sets the font size to font ID #4 for the On and Off states of buttons with the variable text range of 500-504 & 510-515.

NOTE

The Font ID is generated by TPD4 and is located in TPD4 through the Main menu.
Panel > Generate Programmer's Report >Text Only Format >Readme.txt.

"^" Button Commands (Cont.)	
^GDI Change the bargraph drag increment.	Syntax: "'^GDI-<vt addr range>,<bargraph drag increment>'" Variable: variable text address range = 1 - 4000. bargraph drag increment = The default drag increment is 256. Example: SEND_COMMAND Panel,"'^GDI-7,128'" Sets the bargraph with variable text 7 to a drag increment of 128.
^GIV Invert the joystick axis to move the origin to another corner.	Parameters 1,2, and 3 will cause a bargraph or slider to be inverted regardless of orientation. Their effect will be as described for joysticks. Syntax: "'^GIV-<vt addr range>,<joystick axis to invert>'" Variable: variable text address range = 1 - 4000. joystick axis to invert = 0 - 3. 0 1 2 3 0 = Normal 1 = Invert horizontal axis 2 = Invert vertical axis 3 = Invert both axis locations For a bargraph 1 = Invert , 0 = Non Invert Example: SEND_COMMAND Panel,"'^GIV-500,3'" Inverts the joystick axis origin to the bottom right corner.
^GLH Change the bargraph upper limit.	Syntax: "'^GLH-<vt addr range>,<bargraph hi>'" Variable: variable text address range = 1 - 4000. bargraph limit range = 1 - 65535 (*bargraph upper limit range*). Example: SEND_COMMAND Panel,"'^GLH-500,1000'" Changes the bargraph upper limit to 1000.
^GLL Change the bargraph lower limit.	Syntax: "'^GLL-<vt addr range>,<bargraph low>'" Variable: variable text address range = 1 - 4000. bargraph limit range = 1 - 65535 (*bargraph lower limit range*). Example: SEND_COMMAND Panel,"'^GLL-500,150'" Changes the bargraph lower limit to 150.

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^GRD
Change the bargraph ramp-down time in 1/10th of a second.</td><td>Syntax:
"'^GRD-<vt addr range>,<bargraph ramp down time>'"
Variable:
variable text address range = 1 - 4000.
bargraph ramp down time = In 1/10th of a second intervals.
Example:
SEND_COMMAND Panel,"'^GRD-500,200'"
Changes the bargraph ramp down time to 20 seconds.</td></tr>
<tr><td>^GRU
Change the bargraph ramp-up time in 1/10th of a second.</td><td>Syntax:
"'^GRU-<vt addr range>,<bargraph ramp up time>'"
Variable:
variable text address range = 1 - 4000.
bargraph ramp up time = In 1/10th of a second intervals.
Example:
SEND_COMMAND Panel,"'^GRU-500,100'"
Changes the bargraph ramp up time to 10 seconds.</td></tr>
<tr><td>^GSC
Change the bargraph slider color or joystick cursor color.</td><td>A user can also assign the color by Name and R,G,B value (RRGGBB or RRGGBBAA).
Syntax:
"'^GSC-<vt addr range>,<color value>'"
Variable:
variable text address range = 1 - 4000.
color value = Refer to theRGB Values for all 88 Basic Colors table on page 141.
Example:
SEND_COMMAND Panel,"'^GSC-500,12'"
Changes the bargraph or joystick slider color to Yellow.</td></tr>
<tr><td>^GSN
Change the bargraph slider name or joystick cursor name.</td><td>Slider names and cursor names can be found in the TPDesign4 slider name and cursor drop-down list.
Syntax:
"'^GSN-<vt addr range>,<bargraph slider name>'"
Variable:
variable text address range = 1 - 4000.
bargraph slider name = See table below.
<table><tr><td colspan="3">Bargraph Slider Names:</td></tr><tr><td>None</td><td>Ball</td><td>Circle -L</td></tr><tr><td>Circle -M</td><td>Circle -S</td><td>Precision</td></tr><tr><td>Rectangle -L</td><td>Rectangle -M</td><td>Rectangle -S</td></tr><tr><td>Windows</td><td>Windows Active</td><td></td></tr><tr><td colspan="3">Joystick Cursor Names:</td></tr><tr><td>None</td><td>Arrow</td><td>Ball</td></tr><tr><td>Circle</td><td>Crosshairs</td><td>Gunsight</td></tr><tr><td>Hand</td><td>Metal</td><td>Spiral</td></tr><tr><td>Target</td><td>View Finder</td><td></td></tr></table>Example:
SEND_COMMAND Panel,"'^GSN-500,Ball'"
Changes the bargraph slider name or the Joystick cursor name to 'Ball'.</td></tr>
</table>

"^" Button Commands (Cont.)	

^ICO
Set the icon to a button.
	Syntax:
	`"'^ICO-<vt addr range>,<button states range>,<icon index>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	icon index range = 0 - 9900 (**a value of 0 is clear**).
	Example:
	`SEND_COMMAND Panel,"'^ICO-500.504&510.515,1&2,1'"`
	Sets the icon for On and Off states for buttons with variable text ranges of 500-504 & 510-515.

^JSB
Set bitmap/ picture alignment using a numeric keypad layout for those buttons with a defined address range.
	The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.
	Syntax:
	`"'^JSB-<vt addr range>,<button states range>,<new text alignment>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text alignment = Value of 1 - 9 corresponds to the following locations:
	0
	1 2 3
	4 5 6
	7 8 9
	Zero can be used for an absolute position
	Example:
	`SEND_COMMAND Panel,"'^JSB-500.504&510.515,1&2,1'"`
	Sets the off/on state picture alignment to upper left corner for those buttons with variable text ranges of 500-504 & 510-515.

^JSI
Set icon alignment using a numeric keypad layout for those buttons with a defined address range.
	The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.
	Syntax:
	`"'^JSI-<vt addr range>,<button states range>,<new icon alignment>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new icon alignment = Value of 1 - 9 corresponds to the following locations:
	0
	1 2 3
	4 5 6
	7 8 9
	Zero can be used for an absolute position
	Example:
	`SEND_COMMAND Panel,"'^JSI-500.504&510.515,1&2,1'"`
	Sets the Off/On state icon alignment to upper left corner for those buttons with variable text range of 500-504 & 510-515.

"^" Button Commands (Cont.)	

^JST
Set text alignment using a numeric keypad layout for those buttons with a defined address range.
	The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.
	Syntax:
	`"'^JST-<vt addr range>,<button states range>,<new text alignment>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text alignment = Value of 1 - 9 corresponds to the following locations:
	0
	1 2 3
	4 5 6
	7 8 9
	Zero can be used for an absolute position
	Example:
	`SEND_COMMAND Panel,"'^JST-500.504&510.515,1&2,1'"`
	Sets the text alignment to the upper left corner for those buttons with variable text ranges of 500-504 & 510-515.

^MBT
Set the Mouse Button mode On for the virtual PC.
	Syntax:
	`"'^MBT-<pass data>'"`
	Variable:
	pass data:
	0 = None
	1 = Left
	2 = Right
	3 = Middle
	Example:
	`SEND COMMAND Panel,"'^MBT-1'"`
	Sets the mouse button mode to 'Left Mouse Click'.

^MDC
Turn On the 'Mouse double-click' feature for the virtual PC.
	Syntax:
	`"'^MDC'"`
	Example:
	`SEND COMMAND Panel,"'^MDC'"`
	Sets the mouse double-click for use with the virtual PC.

^SHO
Show or hide a button with a set variable text range.
	Syntax:
	`"'^SHO-<vt addr range>,<command value>'"`
	Variable:
	variable text address range = 1 - 4000.
	command value = (0= hide, 1= show).
	Example:
	`SEND_COMMAND Panel,"'^SHO-500.504&510.515,0'"`
	Hides buttons with variable text address range 500-504 & 510-515.

"^" Button Commands (Cont.)	

^TEC
Set the text effect color for the specified addresses/states to the specified color.
	The Text Effect is specified by name and can be found in TPD4. You can also assign the color by name or RGB value (RRGGBB or RRGGBBAA).
	Syntax:
	`"'^TEC-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to theRGB Values for all 88 Basic Colors table on page 141.
	Example:
	`SEND_COMMAND Panel,"'^TEC-500.504&510.515,1&2,12'"`
	Sets the text effect color to Very Light Yellow on buttons with variable text 500-504 and 510-515.

^TEF
Set the text effect.
	The Text Effect is specified by name and can be found in TPD4.
	Syntax:
	`"'^TEF-<vt addr range>,<button states range>,<text effect name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	text effect name = **Refer to theText Effects table on page 166 for a listing of text effect names**.
	Example:
	`SEND_COMMAND Panel,"'^TEF-500.504&510.515,1&2,Soft Drop Shadow 3'"`
	Sets the text effect to Soft Drop Shadow 3 for the button with variable text range 500-504 and 510-515.

^TXT
Assign a text string to those buttons with a defined address range.
	Sets Non-Unicode text.
	Syntax:
	`"'^TXT-<vt addr range>,<button states range>,<new text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^TXT-500.504&510.515,1&2,Test Only'"`
	Sets the On and Off state text for buttons with the variable text ranges of 500-504 & 510-515.

"^" Button Commands (Cont.)	

^UNI
Set Unicode text.
	For the ^UNI command (%UN and ^BMF command), the Unicode text is sent as ASCII-HEX nibbles.
	Syntax:
	`"'^UNI-<vt addr range>,<button states range>,<unicode text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	unicode text = Unicode HEX value.
	Example:
	`SEND_COMMAND Panel,"'^UNI-500,1,0041'"`
	Sets the button's unicode character to 'A'.
	Note: To send the variable text 'A' in unicode to all states of the variable text button 1, (for which the character code is 0041 Hex), send the following command:
	`SEND_COMMAND TP,"'^UNI-1,0,0041'"`
	Note: Unicode is always represented in a HEX value. TPD4 generates (through the Text Enter Box dialog) unicode HEX values. Refer to the TPDesign4 Instruction Manual for more information.

Text Effect Names

The following is a listing of text effects names. This list is associated with the **^TEF** command on page 164.

Text Effects	
• Glow -S	• Hard Drop Shadow 6
• Glow -M	• Hard Drop Shadow 7
• Glow -L	• Hard Drop Shadow 8
• Glow -X	• Soft Drop Shadow 1 with outline
• Outline -S	• Soft Drop Shadow 2 with outline
• Outline -M	• Soft Drop Shadow 3 with outline
• Outline -L	• Soft Drop Shadow 4 with outline
• Outline -X	• Soft Drop Shadow 5 with outline
• Soft Drop Shadow 1	• Soft Drop Shadow 6 with outline
• Soft Drop Shadow 2	• Soft Drop Shadow 7 with outline
• Soft Drop Shadow 3	• Soft Drop Shadow 8 with outline
• Soft Drop Shadow 4	• Medium Drop Shadow 1 with outline
• Soft Drop Shadow 5	• Medium Drop Shadow 2 with outline
• Soft Drop Shadow 6	• Medium Drop Shadow 3 with outline
• Soft Drop Shadow 7	• Medium Drop Shadow 4 with outline
• Soft Drop Shadow 8	• Medium Drop Shadow 5 with outline
• Medium Drop Shadow 1	• Medium Drop Shadow 6 with outline
• Medium Drop Shadow 2	• Medium Drop Shadow 7 with outline
• Medium Drop Shadow 3	• Medium Drop Shadow 8 with outline
• Medium Drop Shadow 4	• Hard Drop Shadow 1 with outline
• Medium Drop Shadow 5	• Hard Drop Shadow 2 with outline
• Medium Drop Shadow 6	• Hard Drop Shadow 3 with outline
• Medium Drop Shadow 7	• Hard Drop Shadow 4 with outline
• Medium Drop Shadow 8	• Hard Drop Shadow 5 with outline
• Hard Drop Shadow 1	• Hard Drop Shadow 6 with outline
• Hard Drop Shadow 2	• Hard Drop Shadow 7 with outline
• Hard Drop Shadow 3	• Hard Drop Shadow 8 with outline
• Hard Drop Shadow 4	
• Hard Drop Shadow 5	

Button Query Commands

Button Query commands reply back with a custom event. There will be one custom event for each button/state combination. Each query is assigned a unique custom event type. **The following example is for debug purposes only:**

```
NetLinx Example: CUSTOM_EVENT[device, Address, Custom event type]
```

DEFINE_EVENT

```
CUSTOM_EVENT[TP,529,1001]       // Text
CUSTOM_EVENT[TP,529,1002]       // Bitmap
CUSTOM_EVENT[TP,529,1003]       // Icon
CUSTOM_EVENT[TP,529,1004]       // Text Justification
CUSTOM_EVENT[TP,529,1005]       // Bitmap Justification
CUSTOM_EVENT[TP,529,1006]       // Icon Justification
CUSTOM_EVENT[TP,529,1007]       // Font
CUSTOM_EVENT[TP,529,1008]       // Text Effect Name
CUSTOM_EVENT[TP,529,1009]       // Text Effect Color
CUSTOM_EVENT[TP,529,1010]       // Word Wrap
CUSTOM_EVENT[TP,529,1011]       // ON state Border Color
CUSTOM_EVENT[TP,529,1012]       // ON state Fill Color
CUSTOM_EVENT[TP,529,1013]       // ON state Text Color
CUSTOM_EVENT[TP,529,1014]       // Border Name
CUSTOM_EVENT[TP,529,1015]       // Opacity
```

```
{
   Send_String 0,"'ButtonGet Id=',ITOA(CUSTOM.ID),' Type=',ITOA(CUSTOM.TYPE)"
   Send_String 0,"'Flag   =',ITOA(CUSTOM.FLAG)"
   Send_String 0,"'VALUE1 =',ITOA(CUSTOM.VALUE1)"
   Send_String 0,"'VALUE2 =',ITOA(CUSTOM.VALUE2)"
   Send_String 0,"'VALUE3 =',ITOA(CUSTOM.VALUE3)"
   Send_String 0,"'TEXT   =',CUSTOM.TEXT"
   Send_String 0,"'TEXT LENGTH =',ITOA(LENGTH_STRING(CUSTOM.TEXT))"
}
```

All custom events have the following 6 fields:

Custom Event Fields	
Field	Description
Uint Flag	0 means text is a standard string, 1 means Unicode encoded string
slong value1	button state number
slong value2	actual length of string (this is not encoded size)
slong value3	index of first character (usually 1 or same as optional index
string text	the text from the button
text length (string encode)	button text length

These fields are populated differently for each query command. The text length (String Encode) field is not used in any command.

Button Query Commands	

?BCB
Get the current border color.
	Syntax:
	`"'?BCB-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1011:**
	Flag - zero
	Value1 - Button state number
	Value2 - Actual length of string (should be 9)
	Value3 - Zero
	Text - Hex encoded color value (ex: #000000FF)
	Text length - Color name length (should be 9)
	Example:
	`SEND COMMAND Panel,"'?BCB-529,1'"`
	Gets the button 'OFF state' border color. information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1011
	Flag = 0
	VALUE1 = 1
	VALUE2 = 9
	VALUE3 = 0
	TEXT = #222222FF
	TEXT LENGTH = 9

Button Query Commands (Cont.)	

?BCF
Get the current fill color.
	Syntax:
	`"'?BCF-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1012:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Actual length of string (should be 9)
	Value3 - Zero
	Text - Hex encoded color value (ex: #000000FF)
	Text length - Color name length (should be 9)
	Example:
	`SEND COMMAND Panel,"'?BCF-529,1'"`
	Gets the button 'OFF state' fill color information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1012
	Flag = 0
	VALUE1 = 1
	VALUE2 = 9
	VALUE3 = 0
	TEXT = #FF8000FF
	TEXT LENGTH = 9

?BCT
Get the current text color.
	Syntax:
	`"'?BCT-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1013:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Actual length of string (should be 9)
	Value3 - Zero
	Text - Hex encoded color value (ex: #000000FF)
	Text length - Color name length (should be 9)
	Example:
	`SEND COMMAND Panel,"'?BCT-529,1'"`
	Gets the button 'OFF state' text color information.
	The result sent to Master would be:
	ButtonGet Id = 529 Type = 1013
	Flag = 0
	VALUE1 = 1
	VALUE2 = 9
	VALUE3 = 0
	TEXT = #FFFFFEFF
	TEXT LENGTH = 9

Button Query Commands (Cont.)	

?BMP
Get the current bitmap name.
	Syntax:
	`"'?BMP-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1002:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Actual length of string
	Value3 - Zero
	Text - String that represents the bitmap name
	Text length - Bitmap name text length (should be 9)
	Example:
	`SEND COMMAND Panel,"'?BMP-529,1'"`
	Gets the button 'OFF state' bitmap information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1002
	Flag = 0
	VALUE1 = 1
	VALUE2 = 9
	VALUE3 = 0
	TEXT = Buggs.png
	TEXT LENGTH = 9

?BOP
Get the overall button opacity.
	Syntax:
	`"'?BOP-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1015:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Opacity
	Value3 - Zero
	Text - Blank
	Text length - Zero
	Example:
	`SEND COMMAND Panel,"'?BOP-529,1'"`
	Gets the button 'OFF state' opacity information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1015
	Flag = 0
	VALUE1 = 1
	VALUE2 = 200
	VALUE3 = 0
	TEXT =
	TEXT LENGTH = 0

Button Query Commands (Cont.)	

?BRD
Get the current border name.
	Syntax:
	`"'?BRD-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1014:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Actual length of string
	Value3 - Zero
	Text - String that represents border name
	Text length - Border name length
	Example:
	`SEND COMMAND Panel,"'?BRD-529,1'"`
	Gets the button 'OFF state' border information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1014
	Flag = 0
	VALUE1 = 1
	VALUE2 = 22
	VALUE3 = 0
	TEXT = Double Bevel Raised -L
	TEXT LENGTH = 22

?BWW
Get the current word wrap flag status.
	Syntax:
	`"'?BWW-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1010:**
	Flag - Zero
	Value1 - Button state number
	Value2 - 0 = no word wrap, 1 = word wrap
	Value3 - Zero
	Text - Blank
	Text length - Zero
	Example:
	`SEND COMMAND Panel,"'?BWW-529,1'"`
	Gets the button 'OFF state' word wrap flag status information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1010
	Flag = 0
	VALUE1 = 1
	VALUE2 = 1
	VALUE3 = 0
	TEXT =
	TEXT LENGTH = 0

Button Query Commands (Cont.)	
?FON Get the current font index.	Syntax: "'?FON-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1007:** Flag - Zero Value1 - Button state number Value2 - Font index Value3 - Zero Text - Blank Text length - Zero Example: SEND COMMAND Panel,"'?FON-529,1'" Gets the button 'OFF state' font type index information. The result sent to the Master would be: ButtonGet Id = 529 Type = 1007 Flag = 0 VALUE1 = 1 VALUE2 = 72 VALUE3 = 0 TEXT = TEXT LENGTH = 0
?ICO Get the current icon index.	Syntax: "'?ICO-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1003:** Flag - Zero Value1 - Button state number Value2 - Icon Index Value3 - Zero Text - Blank Text length - Zero Example: SEND COMMAND Panel,"'?ICO-529,1&2'" Gets the button 'OFF state' icon index information. The result sent to the Master would be: ButtonGet Id = 529 Type = 1003 Flag = 0 VALUE1 = 2 VALUE2 = 12 VALUE3 = 0 TEXT = TEXT LENGTH = 0

Button Query Commands (Cont.)	

?JSB
Get the current bitmap justification.
	Syntax:
	`"'?JSB-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1005:**
	Flag - Zero
	Value1 - Button state number
	Value2 - 1 - 9 justify
	Value3 - Zero
	Text - Blank
	Text length - Zero
	Example:
	`SEND COMMAND Panel,"'?JSB-529,1'"`
	Gets the button 'OFF state' bitmap justification information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1005
	Flag = 0
	VALUE1 = 1
	VALUE2 = 5
	VALUE3 = 0
	TEXT =
	TEXT LENGTH = 0

?JSI
Get the current icon justification.
	Syntax:
	`"'?JSI-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1006:**
	Flag - Zero
	Value1 - Button state number
	Value2 - 1 - 9 justify
	Value3 - Zero
	Text - Blank
	Text length - Zero
	Example:
	`SEND COMMAND Panel,"'?JSI-529,1'"`
	Gets the button 'OFF state' icon justification information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1006
	Flag = 0
	VALUE1 = 1
	VALUE2 = 6
	VALUE3 = 0
	TEXT =
	TEXT LENGTH = 0

Button Query Commands (Cont.)	
?JST Get the current text justification.	Syntax: "'?JST-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1004:** Flag - Zero Value1 - Button state number Value2 - 1 - 9 justify Value3 - Zero Text - Blank Text length - Zero Example: SEND COMMAND Panel,"'?JST-529,1'" Gets the button 'OFF state' text justification information. The result sent to the Master would be: ButtonGet Id = 529 Type = 1004 Flag = 0 VALUE1 = 1 VALUE2 = 1 VALUE3 = 0 TEXT = TEXT LENGTH = 0
?TEC Get the current text effect color.	Syntax: "'?TEC-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1009:** Flag - Zero Value1 - Button state number Value2 - Actual length of string (should be 9) Value3 - Zero Text - Hex encoded color value (ex: #000000FF) Text length - Color name length (should be 9) Example: SEND COMMAND Panel,"'?TEC-529,1'" Gets the button 'OFF state' text effect color information. The result sent to the Master would be: ButtonGet Id = 529 Type = 1009 Flag = 0 VALUE1 = 1 VALUE2 = 9 VALUE3 = 0 TEXT = #5088F2AE TEXT LENGTH = 9

Button Query Commands (Cont.)	

?TEF
Get the current text effect name.
	Syntax:
	`"'?TEF-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1008:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Actual length of string
	Value3 - Zero
	Text - String that represents the text effect name
	Text length - Text effect name length
	Example:
	`SEND COMMAND Panel,"'?TEF-529,1'"`
	Gets the button 'OFF state' text effect name information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1008
	Flag = 0
	VALUE1 = 1
	VALUE2 = 18
	VALUE3 = 0
	TEXT = Hard Drop Shadow 3
	TEXT LENGTH = 18

?TXT
Get the current text information.
	Syntax:
	`"'?TXT-<vt addr range>,<button states range>,<optional index>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	optional index = This is used if a string was too long to get back in one command. The reply will start at this index.
	custom event type **1001:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Actual length of string
	Value3 - Index
	Text - Text from the button
	Text length - Button text length
	Example:
	`SEND COMMAND Panel,"'?TXT-529,1'"`
	Gets the button 'OFF state' text information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1001
	Flag = 0
	VALUE1 = 1
	VALUE2 = 14
	VALUE3 = 1
	TEXT = This is a test
	TEXT LENGTH = 14

Panel Runtime Operations

Serial Commands are used in the AxcessX Terminal Emulator mode. These commands are case insensitive.

Panel Runtime Operation Commands	

ABEEP
Output a single beep even if beep is Off.
	Syntax:
	`"'ABEEP'"`
	Example:
	`SEND COMMAND Panel,"'ABEEP'"`
	Outputs a beep of duration 1 beep even if beep is Off.

ADBEEP
Output a double beep even if beep is Off.
	Syntax:
	`"'ADBEEP'"`
	Example:
	`SEND COMMAND Panel,"'ADBEEP'"`
	Outputs a double beep even if beep is Off.

@AKB
Pop up the keyboard icon and initialize the text string to that specified.
	Keyboard string is set to null on power up and is stored until power is lost. The Prompt Text is optional.
	Syntax:
	`"'@AKB-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@AKB-Texas;Enter State'"`
	Pops up the Keyboard and initializes the text string 'Texas' with prompt text 'Enter State'.

AKEYB
Pop up the keyboard icon and initialize the text string to that specified.
	Keyboard string is set to null on power up and is stored until power is lost.
	Syntax:
	`"'AKEYB-<initial text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'AKEYB-This is a Test'"`
	Pops up the Keyboard and initializes the text string 'This is a Test'.

AKEYP
Pop up the keypad icon and initialize the text string to that specified.
	The keypad string is set to null on power up and is stored until power is lost.
	Syntax:
	`"'AKEYP-<number string>'"`
	Variables:
	`number string = 0 - 9999.`
	Example:
	`SEND COMMAND Panel,"'AKEP-12345'"`
	Pops up the Keypad and initializes the text string '12345'.

AKEYR
Remove the Keyboard/ Keypad.
	Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands.
	Syntax:
	`"'AKEYR'"`
	Example:
	`SEND COMMAND Panel,"'AKEYR'"`
	Removes the Keyboard/Keypad.

Panel Runtime Operation Commands (Cont.)	

@AKP
Pop up the keypad icon and initialize the text string to that specified.
	Keypad string is set to null on power up and is stored until power is lost. The Prompt Text is optional.
	Syntax:
	`"'@AKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@AKP-12345678;ENTER PASSWORD'"`
	Pops up the Keypad and initializes the text string '12345678' with prompt text 'ENTER PASSWORD'.

@AKR
Remove the Keyboard/ Keypad.
	Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands.
	Syntax:
	`"'@AKR'"`
	Example:
	`SEND COMMAND Panel,"'@AKR'"`
	Removes the Keyboard/Keypad.

BEEP
Output a beep.
	Syntax:
	`"'BEEP'"`
	Example:
	`SEND COMMAND Panel,"'BEEP'"`
	Outputs a beep.

BRIT
Set the panel brightness.
	Syntax:
	`"'BRIT-<brightness level>'"`
	Variable:
	brightness level = 0 - 100.
	Example:
	`SEND COMMAND Panel,"'BRIT-50'"`
	Sets the brightness level to 50.

@BRT
Set the panel brightness.
	Syntax:
	`"'@BRT-<brightness level>'"`
	Variable:
	brightness level = 0 - 100.
	Example:
	`SEND COMMAND Panel,"'@BRT-70'"`
	Sets the brightness level to 70.

DBEEP
Output a double beep.
	Syntax:
	`"'DBEEP'"`
	Example:
	`SEND COMMAND Panel,"'DBEEP'"`
	Outputs a double beep.

Panel Runtime Operation Commands (Cont.)	

@EKP
Extend the Keypad.
	Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional.
	Syntax:
	`"'@EKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@EKP-33333333;Enter Password'"`
	Pops up the Keypad and initializes the text string '33333333' with prompt text 'Enter Password'.

PKEYP
Present a private keypad.
	Pops up the keypad icon and initializes the text string to that specified. Keypad displays a '*' instead of the numbers typed. The Prompt Text is optional.
	Syntax:
	`"'PKEYP-<initial text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'PKEYP-123456789'"`
	Pops up the Keypad and initializes the text string '123456789' in '*'.

@PKP
Present a private keypad.
	Pops up the keypad icon and initializes the text string to that specified. Keypad displays a '*' instead of the numbers typed. The Prompt Text is optional.
	Syntax:
	`"'@PKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@PKP-1234567;ENTER PASSWORD'"`
	Pops up the Keypad and initializes the text string 'ENTER PASSWORD' in '*'.

SETUP
Send panel to SETUP page.
	Syntax:
	`"'SETUP'"`
	Example:
	`SEND COMMAND Panel,"'SETUP'"`
	Sends the panel to the Setup Page.

SHUTDOWN
Shut down the batteries providing power to the panel.
	Syntax:
	`"'SHUTDOWN'"`
	Example:
	`SEND COMMAND Panel,"'SHUTDOWN'"`
	Shuts-down the batteries feeding power to the panel. This function saves the battery from discharging.

SLEEP
Force the panel into screen saver mode.
	Syntax:
	`"'SLEEP'"`
	Example:
	`SEND COMMAND Panel,"'SLEEP'"`
	Forces the panel into screen saver mode.

Panel Runtime Operation Commands (Cont.)	

@SOU
Play a sound file.
	Syntax:
	`"'@SOU-<sound name>'"`
	Variables:
	`sound name = Name of the sound file. Supported sound file formats are: WAV & MP3.`
	Example:
	`SEND COMMAND Panel,"'@SOU-Music.wav'"`
	Plays the 'Music.wav' file.

@TKP
Present a telephone keypad.
	Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional.
	Syntax:
	`"'@TKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@TKP-999.222.1211;Enter Phone Number'"`
	Pops-up the Keypad and initializes the text string '999.222.1211' with prompt text 'Enter Phone Number'.

TPAGEON
Turn On page tracking.
	This command turns On page tracking, whereby when the page or popups change, a string is sent to the Master. This string may be captured with a CREATE_BUFFER command for one panel and sent directly to another panel.
	Syntax:
	`"'TPAGEON'"`
	Example:
	`SEND COMMAND Panel,"'TPAGEON'"`
	Turns On page tracking.

TPAGEOFF
Turn Off page tracking.
	Syntax:
	`"'TPAGEOFF'"`
	Example:
	`SEND COMMAND Panel,"'TPAGEOFF'"`
	Turns Off page tracking.

@VKB
Popup the virtual keyboard.
	Syntax:
	`"'@VKB'"`
	Example:
	`SEND COMMAND Panel,"'@VKB'"`
	Pops-up the virtual keyboard.

WAKE
Force the panel out of screen saver mode.
	Syntax:
	`"'WAKE'"`
	Example:
	`SEND COMMAND Panel,"'WAKE'"`
	Forces the panel out of the screen saver mode.

Input Commands

These Send Commands are case insensitive.

Input Commands	

^CAL
Put panel in calibration mode.
	Syntax:
	`"'^CAL'"`
	Example:
	`SEND COMMAND Panel,"'^CAL'"`
	Puts the panel in calibration mode.

^KPS
Set the keyboard passthru.
	Syntax:
	`"'^KPS-<pass data>'"`
	Variable:
	pass data:
	<blank/empty> = Disables the keyboard.
	0 = Pass data to G4 application (default). This can be used with VPC or text areas.
	1 - 4 = Not used.
	5 = Sends out data to the Master.
	Example:
	`SEND COMMAND Panel,"'^KPS-5'"`
	Sets the keyboard passthru to the Master. Option 5 sends keystrokes directly to the Master via the Send Output String mechanism. This process sends a virtual keystroke command (^VKS) to the Master.
	Example 2:
	`SEND COMMAND Panel,"'^KPS-0'"`
	Disables the keyboard passthru to the Master.
	The following point defines how the parameters within this command work:
	• Accepts keystrokes from any of these sources: attached USB keyboard or Virtual keyboard.

^VKS
Send one or more virtual key strokes to the G4 application.
	Key presses and key releases are not distinguished except in the case of CTRL, ALT, and SHIFT.
	Refer to theEmbedded Codes table on page 181 that define special characters which can be included with the string but may not be represented by the ASCII character set.
	Syntax:
	`"'^VKS-<string>'"`
	Variable:
	string = Only 1 string per command/only one stroke per command.
	Example:
	`SEND COMMAND Panel,"'^VKS-'8"`
	Sends out the keystroke 'backspace' to the G4 application.

Embedded codes

The following is a list of G4 compatible embedded codes:

Embedded Codes		
Decimal numbers	Hexidecimal values	Virtual keystroke
8	($08)	Backspace
13	($0D)	Enter
27	($1B)	ESC
128	($80)	CTRL key down
129	($81)	ALT key down
130	($82)	Shift key down
131	($83)	F1
132	($84)	F2
133	($85)	F3
134	($86)	F4
135	($87)	F5
136	($88)	F6
137	($89)	F7
138	($8A)	F8
139	($8B)	F9
140	($8C)	F10
141	($8D)	F11
142	($8E)	F12
143	($8F)	Num Lock
144	($90)	Caps Lock
145	($91)	Insert
146	($92)	Delete
147	($93)	Home
148	($94)	End
149	($95)	Page Up
150	($96)	Page Down
151	($97)	Scroll Lock
152	($98)	Pause
153	($99)	Break
154	($9A)	Print Screen
155	($9B)	SYSRQ
156	($9C)	Tab
157	($9D)	Windows
158	($9E)	Menu
159	($9F)	Up Arrow
160	($A0)	Down Arrow
161	($A1)	Left Arrow
162	($A2)	Right Arrow
192	($C0)	CTRL key up
193	($C1)	ALT key up
194	($C2)	Shift key up

Panel Setup Commands

These commands are case insensitive.

Panel Setup Commands	
^MUT Set the panel mute state.	Syntax: "'^MUT-<mute state>'" Variable: mute state= 0 = Mute Off and 1 = Mute On. Example: SEND_COMMAND Panel,"'^MUT-1'" Sets the panel's master volume to mute.
@PWD Set the page flip password.	@PWD sets the level 1 password only. Syntax: "'@PWD-<page flip password>'" Variables: page flip password = 1 - 50 ASCII characters. Example: SEND COMMAND Panel,"'@PWD-Main'" Sets the page flip password to 'Main'.
^PWD Set the page flip password.	Password level is required and must be 1 - 4. Syntax: "'^PWD-<password level>,<page flip password>'" Variables: password level = 1 - 4. page flip password = 1 - 50 ASCII characters. Example: SEND COMMAND Panel,"'^PWD-1,Main'" Sets the page flip password on Password Level 1 to 'Main'.
@RPP Reset the protected password.	@RPP resets the protected password to its default (1988). Syntax: "'@RPP'" Example: SEND COMMAND Panel,"'@RPP'" Resets the protected Setup page password to '1988'.
^VOL Set the panel volume.	Syntax: "'^VOL-<volume level>'" Variable: volume level = 0 - 100. ***100 is maximum volume setting.*** Example: SEND_COMMAND Panel,"'^VOL-50'" Sets the panel volume to 50.

Dynamic Image Commands

The following is a listing and descriptions of Dynamic Image Commands.

Dynamic Image Commands	

^BBR
Set the bitmap of a button to use a particular resource.
	Syntax:
	`"'^BBR-<vt addr range>,<button states range>,<resource name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	resource name = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^BBR-700,1,Sports_Image'"`
	Sets the resource name of the button to 'Sports_Image'.

^RAF	See page 184.

^RFR
Force a refresh for a given resource.
	Syntax:
	`"'^RFR-<resource name>'"`
	Variable:
	resource name = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^RFR-Sports_Image'"`
	Forces a refresh on 'Sports_Image'.

^RMF
Modify an existing resource.
	Syntax:
	`"'^RMF-<resource name>,<data>'"`
	Variable:
	resource name = 1 - 50 ASCII characters
	data = Refer to the table in the RAF command for more information.
	Example:
	`SEND_COMMAND Panel,"'^RMF-Sports_Image,%ALab_Test/Images%Ftest.jpg'"`
	Changes the resource 'Sports_Image' file name to 'test.jpg' and the path to 'Lab_Test/Images'.

^RSR
Change the refresh rate for a given resource.
	Syntax:
	`"'^RSR-<resource name>,<refresh rate>'"`
	Variable:
	resource name = 1 - 50 ASCII characters.
	refresh rate = Measured in seconds.
	Example:
	`SEND_COMMAND Panel,"'^RSR-Sports_Image,5'"`
	Sets the refresh rate to 5 seconds for the given resource ('Sports_Image').

Dynamic Image Commands (Cont.)

^RAF

Add new resources.

Adds any and all resource parameters by sending embedded codes and data.

Syntax:

```
"'^RAF-<resource name>,<data>'"
```

Variable:

resource name = 1 - 50 ASCII characters.

data = Refers to the embedded codes, see table below.

Embedded Codes:

Parameter	Embedded Code	Description
protocol	'%P<0-1>'	Set protocol. HTTP (0) or FTP (1).
user	'%U<user>'	Set Username for authentication.
password	'%S<password>'	Set Password for authentication.
host	'%H<host>'	Set Host Name (fully qualified DNS or IP Address).
file	'%F<file>'	Full path to the location of the file or program that will return the resource. The path must be a valid HTTP URL minus the protocol and host. The only exception to this is the inclusion of special escape sequences and in the case of the FTP protocol, regular expressions.
path	'%A<path>'	Set Directory path. The path must be a valid HTTP URL minus the protocol, host, and filename. The only exception to this is the inclusion of special escape sequences and in the case of the FTP protocol, regular expressions.
refresh	'%R<refresh 1-65535>'	The number of seconds between refreshes in which the resource is downloaded again. Refreshing a resource causes the button displaying that resource to refresh also. The default value is 0 (only download the resource once).
newest	'%N<0-1>'	Set the newest file. A value of 1 means that only the most recent file matching the pattern is downloaded.
preserve	'%V<0-1>'	Set the value of the preserve flag. Default is 0. Currently preserve has no function.

Example:

```
SEND_COMMAND Panel,"'^RAF-New Image,%P0%HAMX.COM%ALab/
Test_file%Ftest.jpg'"
```

Adds a new resource. The resource name is 'New Image', %P (protocol) is an HTTP, %H (host name) is ***AMX.COM***, %A (file path) is Lab/Test file, and %F (file name) is ***test.jpg***.

Troubleshooting

This section describes the solutions to possible hardware/firmware issues that could arise during the common operation of a Modero touch panel.

Troubleshooting Information	
Symptom	Solution
My USB drivers has a yellow exclamation point and doesn't appear to be working.	The USB driver was incorrectly installed and should be re-installed: • Power up the panel without the USB cable connected to the panel. • Plug in the USB cable into the G4 panel. You should see a USB icon show up in the System Tray. • Double click on the icon to bring up the list of USB devices (you should see the "AMX USB LAN LINK" device in the list). • If the "Install Driver" dialog doesn't appear automatically, select the "Properties" button and then the "Update Driver" button. • When the Install Driver dialog does appear, click Next to accept all the default prompts. • The OS will notify you that the driver you are installing/updating does not have a digital signature. This is acceptable, agree to continue the installation. • After installation is complete, the exclamation point should disappear.
When using G4 WebControl to communicate with a target panel, a VNC Server dialog appears on my screen.	• During a WebControl connection to a target panel you are prompted with a G4 Authentication dialog which asks you to enter the assigned password for the panel (before gaining access). • If you are ever prompted with a VNC Server dialog, you must enter the IP Address of the target panel. This can be found within the **Setup** > **Protected Setup** > System Settings page. - This IP Address of the panel appears within the IP Settings section of this page • Enter the IP Address and click **OK**. You will then be prompted with the G4 Authentication popup where you must enter the panel's WebControl password.
While attempting to communicate directly with the Virtual Master (on the PC) via a USB connection, I can't get my communication icon to turn Green.	• A Green communication icon indicates that a connection has been established to the target Master or target Virtual Master. • Launch NetLinx Studio and configure the Master Connection communication settings for a Virtual Master. • Navigate to the System Settings page and toggle the *Type* field to **USB**. • Make sure the Type-A USB connector is securely connected to the PC. • Make sure the panel DOESN'T have the mini-USB connected and TURN OFF the panel. • Once the panel has turned ON THEN connect the mini-USB to the Program Port. The USB icon should appear in your system tray. If it doesn't, refer to the *Configuring and Using USB with a Virtual Master* section on page 53. • The panel can take a few minutes to detect the connection to the PC.

Troubleshooting Information (Cont.)	
Symptom	Solution
I updated my panel firmware but my Battery Base page doesn't seem to be working properly.	• Cycle power manually to the panel and check the Battery Base page after startup. • Verify that you are using the most current v2.XX Modero firmware. • If downloading the firmware to the panel via a COM port, try using an IP Address and retry the download of the firmware to the panel.
My Modero panel isn't appearing in my Workspace window.	• Verify that the System number is the same on both the NetLinx Workspace window and the System Settings page on the Modero panel. • Verify you have entered the proper NetLinx Master IP and connection methods into the Master Connection section of the System Settings page.
My Modero panel can't obtain a DHCP Address	In requesting a DHCP Address, the DHCP Server can take up to a few minutes to provide the address. • Verify there is an active Ethernet connection attached to the rear of the Modero before beginning these procedures. • Select **Diagnostics** > **Network Address**, from the Main menu and verify the System number. • If the IP Address field is still empty, give the Modero a few minutes to negotiate a DHCP Address and try again.
My NXT-BP battery pack is blinking when I check the battery life indicator.	• A blinking battery life LED indicates that there is less than 10% power charge remaining on the battery. • It is recommended that you fully charge the battery either in the NXA-BASE/1 battery base or in the NXT-CHG battery charger. • Refer to the *NXA-BASE/1 Battery Base Kit (FG2255-05K)* section on page 28 and *NXT-CHG Battery Charger Kit (FG2255-50K)* section on page 32 for more information.
My panel is not showing up in the Virtual Master's System list of connected devices.	If you a Virtual Master has already connected to the target panel, the G4 device retains the information of the previous Virtual Master System number. • Reboot the panel without the USB cable plugged into the panel. • Configure NetLinx Studio for a Virtual Master connection. Note the System Number used in the Edit Settings window. • Stop communication on the Virtual Master by going to **Settings** > **Stop Communications**. • Click **Yes** to stop communication. • Select the System Number (from the Online Tree tab) and use a right mouse click to select **Refresh System**. This re-establishes communication with the Virtual Master. • Plug-in the mini-USB cable into the corresponding port on the panel. • Wait a few seconds and refresh the system. This re-establishes communication with the Virtual Master. The panel should now appear in the list of available devices.

Troubleshooting Information (Cont.)	
Symptom	Solution
My Connection Status button isn't blinking and it says the USB is connecting.	"USB Connecting" is displayed when the panel is trying to establish USB communication with the PC (either within the NetLinx Studio or TPDesign4 applications). • Remove the USB connector from the panel and close any AMX applications. • Reboot the panel. • Launch the AMX application and attempt reconnect to the panel. • If using Studio for Virtual Master communication, establish a Virtual Master connection, verify the correct System number, stop communication with the Virtual Master, and then re-establish communication by refreshing the system. • After the panel powers-up, reconnect the USB connector to the panel. • Verify that you have a valid USB connection from within your System Tray.
My on-screen mouse cursor doesn't appear.	• The USB connections are not detected until after the particular USB connection plugged into the corresponding port on the panel and power is cycled to the panel.
Calibration is not working.	• After the Modero touch panel has been updated with a new firmware kit (downloaded to the panel through NetLinx Studio), the calibration could need to be reset. • Cycling power to the panel should provide a baseline calibration for the particular touch panel. Proceed to the Calibration page and reset the on-screen calibration.
Panel doesn't respond to my touches	• The protective cover acts to press on the entire LCD and makes calibration difficult because the user can't calibrate on specific crosshairs when the sheet is pressing on the whole LCD. • Verify that the protective laminate coating on the LCD is removed before beginning any calibration process.
There is a crawling, dashed line on the left border of the graphics.	• On some units at some resolutions, there are wavy lines across the entire screen. This has been seen on middle resolutions and is referred to as the "Mid Range Fallout" problem. • This is due to the graphics controller settings in the firmware. • Update to the latest v2.XX.XX firmware. • Visit the **www.amx.com** > T**ech Center** > **Downloadable Files** > **Firmware Files** > **Modero panels**. Then Download the KIT file to your computer.
I was using the power from PSN, and when I connected my NXA-BASE/1 battery base to the active panel, my screen went blank.	Modero battery bases can not be "hot-swapped" or replaced without powering down the Modero and removing the PSN connector. • If you are currently using a direct power connection to the panel and then wish to connect an NXA-BASE/1. - First, power-down the panel and detach the rear power connection. Then, remove any batteries from within the NXA-BASE/1 and connect the battery base to the underside of the panel. - After connecting the base to the un-powered panel, then run power to the panel by either reconnecting the power cable to the rear of the panel or inserting the NXT-BP batteries into the NXA-BASE/1. • Refer to the *NXA-BASE/1 Battery Base Kit (FG2255-05K)* section on page 28 and *Installing the NXA-BASE/1 below an NXT-CV10 Panel* section on page 30 for more information.

Troubleshooting Information (Cont.)	
Symptom	Solution
I can't seem to completely charge my battery from within an NXA-BASE/1 connected to a powered panel.	NXT-BP batteries can be charged from either an external NXT-CHG battery charger or from within the NXA-BASE/1 located below an NXT panel. • The NXA-BASE/1 Battery base should be updated with the latest firmware (part of the Modero firmware KIT file) from www.amx.com. • The base can only charge the battery while the NXT panel is in Sleep Mode. If the panel parameters are set to their highest values, the priority for the power draw becomes the active panel functions and no power is routed to the base for charging. • Adjust the Display Timeout value to allow the panel to commence the Sleep Mode and begin charging batteries within the base (drawing power from a PSN). • Refer to the *Battery Base Page* section on page 98 for more information.
My WEP doesn't seem to be working.	• WEP will not work unless the same default key is set on both the panel and the Access Point. • For example: if you had your access point set to default key 4 (which was 01:02:03:04:05) you must also set the Modero's panel key 4 to 01:02:03:04:05.
NetLinx Studio only detects one of my connected Masters.	Each Master is give a Device Address of 00000. • Only one Master can be assigned to a particular System number. If you want to work with multiple Masters, open different instances of NetLinx Studio and assign each Master its own System value. • Example: a site has an NXC-ME260/64 and an NI-4000. In order to work with both units. The ME260/64 can be assigned System #1 and the NI-4000 can then be assigned System #2 using two open sessions of NetLinx Studio 2.
I can't seem to connect to a NetLinx Master using my NetLinx Studio 2.x application.	• From the **Settings** > **Master Comm Settings** > **Communication Settings** > **Settings (for TCP/IP)**, uncheck the "**Automatically Ping the Master Controller** to ensure availability". • The pinging is to determine if the Master is available, and to reply with a connection failure instantly if it is not. Without using the ping feature, you will still attempt to make a connection, but a failure will take longer to be recognized. Some firewalls and networks do not allow pinging, though, and the ping will then always result in a failure. • When connecting to a NetLinx Master controller via TCP/IP, the program will first try to ping the controller before attempting a connection. Pinging a device is relatively fast and will determine if the device is off-line, or if the TCP/IP address that was entered was incorrect. If you decide NOT to ping for availability and the controller is off-line, or you have an incorrect TCP/IP address, the program will try for 30-45 seconds to establish a connection. ***Note**:* If you are trying to connect to a master controller that is behind a firewall, you may have to uncheck this option. Most firewalls will not allow ping requests to pass through for security reasons.

Troubleshooting Information (Cont.)	
Symptom	Solution
I have more that one Modero panel connected to my System Master and only one shows up.	Multiple NetLinx Compatible devices (such as Modero panels) can be associated for use with a single Master. Each Modero panel comes with a defaulted Device Number value of 10001. When using multiple panels, it can become very easy to overlook the need to assign different Device Number values to each panel. • Press and hold the grey Front Setup Access button for 3 seconds to open the Setup page. • Press the **Protected Setup** button (located on the lower-left of the panel page), enter ***1988*** into the on-screen Keypad's password field, and press **Done** when finished. • Enter a Device Number value for the panel into the Device Number Keypad. *The default is 10001 and the range is from 1 - 32000*.
After downloading a panel file or firmware to a G4 device, the panel behaves strangely.	Symptoms include: • Having to repeat the download. • Inability to make further downloads to the panel. May get "directory" errors, "graphics hierarchy" errors, etc.… indicating problems with the Compact Flash. • Panel will not boot, or gets stuck on "AMX" splash screen. • Other problems also started after downloading to a new panel or a panel with a TPD4 file that takes up a considerable amount of the available Compact Flash. Cause: • If the G4 device already contains a large enough file, subsequent downloads will take up more space than is available and could often corrupt the Compact Flash. The demo file that typically ships with G4 panels is one such file. Solution: • DO NOT download TPD4 files (of large size) over the demo pages, or any other large TPD4 file. • First download a small blank one page file to the G4 panel using the Normal Transfer option to send/download the page. Reboot the device, then do your regular file or firmware download.
My NXA-BASE/1 Battery Base isn't being recognized by the NXT touch panel.	**The battery base CAN NOT be "hot swapped".** This swapping occurs when an NXT panel is currently being powered by a PSN and then is connected to a battery base containing NXT-BP batteries. Introducing a new power source onto an existing configuration can damage the NXA-BASE. Solution: If your base is not being recognized by the touch panel but is still providing power: • Launch the latest NetLinx Studio. • Refresh the particular System from within the OnLine Tree tab. • Identify the NXT panel using the battery base. • From the Main menu go to **Tools** > **Firmware Transfers** > **Send to NetLinx Device**. • Locate and select the 2255_XXX_**v2_00** KIT file for the battery base. • Enter the Device and System values, verify the method of communication (IP recommended). • Click Send to reload the new base KIT file onto the NXA-BASE/1. If this above steps do not cause the base to be recognized by the NXT touch panel on the Setup page, contact AMX Technical Support for further assistance.

Appendix A

Text Formatting Codes for Bargraphs/Joysticks

Text formatting codes for bargraphs provide a mechanism to allow a portion of a bargraphs text to be dynamically provided information about the current status of the level (multistate and traditional). These codes would be entered into the text field along with any other text.

The following is a code list used for bargraphs:

Bargraph Text Code Inputs		
Code	Bargraph	Multi-State Bargraph
$P	Display the current percentage of the bargraph (derived from the Adjusted Level Value as it falls between the Range Values)	Display the current percentage of the bargraph (derived from the Adjusted Level Value as it falls between the Range Values)
$V	Raw Level Value	Raw Level Value
$L	Range Low Value	Range Low Value
$H	Range High Value	Range High Value
$S	N/A	Current State
$A	Adjusted Level Value (Range Low Value subtracted from the Raw Level Value)	Adjusted Level Value (Range Low Value subtracted from the Raw Level Value)
$R	Low Range subtracted from the High Range	Low Range subtracted from the High Range
$$	Dollar sign	Dollar sign

Buy changing the text on a button (via a VT command) you can modify the codes on a button. When one of the Text Formatting Codes is encountered by the firmware it is replaced with the correct value. These values are derived from the following operations:

Formatting Code Operations	
Code	Operation
$P	(Current Value - Range Low Value / Range High Value - Range Low Value) x 100
$V	Current Level Value
$L	Range Low Value
$H	Range High Value
$S	Current State (if regular bargraph then resolves to nothing)
$A	Current Value - Range Low Value
$R	Range High Value - Range Low Value

Given a current raw level value of 532, a range low value of 500 and a high range value of 600 the following text formatting codes would yield the following strings as shown in the table below:

Example	
Format	Display
$P%	32%
$A out of $R	32 out of 100
$A of 0 - $R	32 of 0 - 100
$V of $L - $H	532 of 500 - 600

Text Area Input Masking

Text Area Input Masking can be used to limit the allowed/correct characters that are entered into a text area. For example, in working with a zip code, a user could limit the entry to a max length of only 5 characters but, with input masking, you could limit them to 5 mandatory numerical digits and 4 optional numerical digits. A possible use for this feature is to enter information into form fields. The purpose of this feature is to:

- Force you to use correct type of characters (i.e. numbers vs. characters)
- Limit the number of characters in a text area
- Suggest proper format with fixed characters
- Right to Left
- Required or Optional
- Change/Force a Case
- Create multiple logical fields
- Specify range of characters/number for each field

With this feature, it is NOT necessary to:

- Limit you to a choice of selections
- Handle complex input tasks such as names, days of the weeks or months by name
- Perform complex validation such as Subnet Mask validation

Input mask character types

These character types define what information is allowed to be entered in any specific instance. The following table lists what characters in an input mask will define what characters are allowed in any given position.

Character Types	
Character	Masking Rule
0	Digit (0 to 9, entry required, plus [+] and minus [-] signs not allowed)
9	Digit or space (entry not required, plus and minus signs not allowed)
#	Digit or space (entry not required; plus and minus signs allowed)
L	Letter (A to Z, entry required)
?	Letter (A to Z, entry optional)
A	Letter or digit (entry required)
a	Letter or digit (entry optional)
&	Any character or a space (entry required)
C	Any character or a space (entry optional)

The number of the above characters used determines the length of the input masking box. Example: 0000 requires an entry, requires digits to be used, and allows only 4 characters to be entered/used.

Refer to the following Send Commands for more detailed information:

- ^BIM - Sets the input mask for the specified addresses. (see the *^BIM* section on page 150).
- ^BMF subcommand **%MK** - sets the input mask of a text area (see the *^BMF* section on page 152).

Input mask ranges

These ranges allow a user to specify the minimum and maximum numeric value for a field. ***Only one range is allowed per field. Using a range implies a numeric entry ONLY.***

Input Mask Ranges	
Character	Meaning
[	Start range
]	End range
|	Range Separator

An example from the above table:

[0|255] This allows a user to enter a value from 0 to 255.

Input mask next field characters

These characters allow you to specify a list of characters that cause the keyboard to move the focus to the next field when pressed instead of inserting the text into the text area.

Input Mask Next Field Char	
Character	Meaning
{	Start Next Field List
}	End Next Field List

An example from the above table:

{.} or {:} or {.:} Tells the system that after a user hits any of these keys, proceed to the next text area input box.

Input mask operations

Input Mask Operators change the behavior of the field in the following way:

Input Mask Operators	
Character	Meaning
<	Forces all characters to be converted to lowercase
>	Forces all characters to be converted to uppercase
^	Sets the overflow flag for this field

Input mask literals

To define a literal character, enter any character, other than those shown in the above table *(including spaces, and symbols)*. A back-slash ('\') causes the character that follows it to be displayed as the literal character. For example, **\A** is displayed just as the letter **A**. To define one of the following characters as a literal character, precede that character with a back-slash. Text entry operation using Input Masks.

A keyboard entry using normal text entry is straightforward. However, once an input mask is applied, the behavior of the keyboard needs to change to accommodate the input mask's requirement. When working with masks, any literal characters in the mask will be "skipped" by any cursor movement including cursor keys, backspace, and delete.

When operating with a mask, the mask should be displayed with placeholders. The "-" character should display where you should enter a character. The arrow keys will move between the "-" characters and allow you to replace them. The text entry code operates as if it is in the overwrite mode. If the cursor is positioned on a character already entered and you type in a new (and valid) character, the new character replace the old character. There is no shifting of characters.

When working with ranges specified by the [] mask, the keyboard allows you to enter a number between the values listed in the ranges. If a user enters a value that is larger than the max, the maximum number of right-most characters is used to create a new, acceptable value.

- **Example 1**: If you type "125" into a field accepting 0-100, then the values displayed will be "1", "12", "25".
- **Example2**: If the max for the filed was 20, then the values displayed will be "1", "12", "5".

When data overflows from a numerical field, the overflow value is added to the previous field on the chain, **if** the overflow character was specified. In the above example, if the overflow flag was set, the first example will place the "1" into the previous logical field and the second example will place "12" in the previous logical field. If the overflow filed already contains a value, the new value will be inserted to the right of the current characters and the overflow field will be evaluated. Overflow continues to work until a filed with no overflow value is set or there are no more fields left (i.e. reached first field).

If a character is typed and that characters appear in the Next Field list, the keyboard should move the focus to the next field. For example, when entering time, a **":"** is used as a next field character. If you hit "1:2", the 1 is entered in the current field (hours) and then the focus is moved to the next field and 2 is entered in that field.

When entering time in a 12-hour format, entry of AM and PM is required. Instead of adding AM/PM to the input mask specification, the AM/PM should be handled within the NetLinx code. This allows a programmer to show/hide and provide discrete feedback for AM and PM.

Input mask output examples

The following are some common input masking examples:

Output Examples		
Common Name	Input Mask	Input
IP Address Quad	[0|255]{.}	Any value from 0 to 255
Hour	[1|12]{:}	Any value from 1 to 12
Minute/Second	[0|59]{:}	Any value from 0 to 59
Frames	[0|29]{:}	Any value from 0 to 29
Phone Numbers	(999) 000-0000	(555) 555-5555
Zip Code	00000-9999	75082-4567

URL Resources

A URL can be broken into several parts. For example: the URL *http://www.amx.com/company-info-home.asp*. This URL indicates that the protocol in use is **http** (HyperText Transport Protocol) and that the information resides on a host machine named **www.amx.com**. The image on that host machine is given an assignment (*by the program*) name of **company-info-home.asp** *(Active Server Page)*.

The exact meaning of this name on the host machine is both protocol dependent and host dependent. The information normally resides in a file, but it could be generated dynamically. This component of the URL is called the file component, even though the information is not necessarily in a file.

A URL can optionally specify a port, which is the port number to which the TCP connection is made on the remote host machine. If the port is not specified, the default port for the protocol is used instead. For example, the default port for http is 80. An alternative port could be specified as: http://www.amx.com:8080/company-info-home.asp.

Any legal HTTP syntax can be used.

Special escape sequences

The system has only a limited knowledge of URL formats in that it transparently passes the URL information onto the server for translation. A user can then pass any parameters to the server side programs such as CGI scripts or active server pages. However; the system will parse the URL looking for special escape codes. When it finds an escape code it replaces that code with a particular piece of panel, button, or state information.
For example, "http://www.amx.com/img.asp?device=$DV" would become "http://www.amx.com/img.asp?device=10001". Other used escape sequences include:

Escape Sequences	
Sequence	Panel Information
$DV	Device Number
$SY	System Number
$IP	IP Address
$HN	Host Name
$MC	Mac Address
$ID	Neuron ID
$PX	X Resolution of current panel mode/file
$PY	Y Resolution of current panel mode/file
$BX	X Resolution of current button
$BY	Y Resolution of current button
$BN	Name of button
$ST	Current state
$AC	Address Code
$AP	Address Port
$CC	Channel Code
$CP	Channel Port
$LC	Level Code
$LP	Level Port

Appendix B - Wireless Technology

Overview of Wireless Technology

- **802.11b/2.4 GHz and 802.11a/5 GHz** are the two major WLAN standards and both operate using radio frequency (RF) technology. Together the two standards are together called Wi-Fi and operate in frequency bands of 2.4 GHz and 5 GHz respectively.
  The ***802.11b*** specification was the first to be finalized and reach the marketplace. The actual throughput you can expect to obtain from an 802.11b network will typically be between 4 and 5 Mbps.
  Because of the higher frequency (and thus shorter wavelength) that they use, ***802.11a*** signals have a much tougher time penetrating solid objects like walls, floors, and ceilings. As a result, the price for 802.11a's higher speed is not only shorter in range but also a weaker and less consistent signal.
  802.11g provides increased bandwidth at 54 Mbps. As part of the IEEE 802.11g specification, when throughput cannot be maintained, this card will automatically switch algorithms in order to maintain the highest spread possible at a given distance. In addition, 802.11g can also step down to utilize 802.11b algorithms and also maintain a connection at longer distances.
- IP Routing is a behavior of the wireless routing is largely dependent on the wired network interface. Although the panel can be connected to two networks simultaneously it may only have one gateway. If the wired network was successfully set up and a gateway was obtained; then the default route for all network traffic will be via the wired network. In the event that the wired network was not configured, then the default route for all network traffic will be via the wireless network. The wired network connection always takes priority.
  - As an example: Imagine a panel connected to two networks A & B. A is the wired network and B is the wireless network. If the Master controller is on either of these networks then it will be reached. However if the Master controller is on a different network, C, then determining which network interface (wired or wireless) that will be used is dependent on the gateway.
- **Wireless Access Points** are the cornerstone of any wireless network. A Wireless Access Point acts as a bridge between a wired and wireless network. It aggregates the traffic from all the wireless clients and forwards it down the network to the switch or router.
  One Wireless Access Point may be all you need. However, you could need more Wireless Access Points depending on either how large your installation is, how it is laid out, and how it is constructed.
- **Wireless Equivalent Privacy** (**WEP**) Security is a method by which WLANs protect wireless data streams. A data stream encrypted with WEP can still be intercepted or eavesdropped upon, but the encryption makes the data unintelligible to the interloper. The strength of WEP is measured by the length of the key used to encrypt the data. The longer the key, the harder it is to crack.
  802.11b implementations provided 64-bit and 128-bit WEP keys. This is known respectively as 64-bit and 128-bit WEP encryption. 64-bit is generally not regarded as adequate security protection. Both key lengths are supported by the Modero product line.
  Whichever level of WEP you use, it's ***crucial to use identical settings (CASE SENSITIVE)***--the key length, and the key itself-- on all devices. Only devices with common WEP settings will be able to communicate. Similarly, if one device has WEP enabled and another doesn't, they won't be able to talk to each other.

Although the calculations required to encrypt data with WEP can impact the performance of your wireless network, it's generally seen only when running benchmarks, and not large enough to be noticeable in the course of normal network usage.

Terminology

- **802.1x**
  - IEEE 802.1x is an IEEE standard that is built on the Internet standard EAP (Extensible Authentication Protocol). 802.1x is a standard for passing EAP messages over either a wired or wireless LAN. Additionally, 802.1x is also responsible for communicating the method with which WAPs and wireless users can share and change encryption keys. This continuous key change helps resolve any major security vulnerabilities native to WEP.
- **AES**
  - Short for Advanced Encryption Standard, is a cipher currently approved by the NSA to protect US Government documents classified as Top Secret. The AES cipher is the first cipher protecting Top Secret information available to the general public.
- **CERTIFICATES (CA)**
  - A certificate can have many forms, but at the most basic level, a certificate is an identity combined with a public key, and then signed by a certification authority. The certificate authority (CA) is a trusted external third party which "signs" or validates the certificate. When a certificate has been signed, it gains some cryptographic properties. AMX supports the following security certificates within three different formats:
    - **PEM** (Privacy Enhanced Mail)
    - **DER** (Distinguished Encoding Rules)
    - **PKCS12** (Public Key Cryptography Standard #12)
  - Typical certificate information can include the following items:
    - Certificate Issue Date
    - Extensions
    - Issuer
    - Public Key
    - Serial Number
    - Signature Algorithm
    - User
    - Version
- **MIC**
  - Short for Message Integrity Check, prevents forged packets from being sent. Through WEP it was possible to alter a packet whose content was known even if it had not been decrypted.

- **TKIP**
  - Short for Temporal Key Integration, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP provides per-packet key mixing, message integrity check and re-keying mechanism, thus ensuring every data packet is sent with its own unique encryption key. Key mixing increases the complexity of decoding the keys by giving the hacker much less data that has been encrypted using any one key.
- **WEP**
  - Short for Wired Equivalent Privacy (WEP), is a scheme used to secure wireless networks (Wi-Fi). A wireless network broadcasts messages using radio which are particularly susceptible to hacker attacks. WEP was intended to provide the confidentiality and security comparable to that of a traditional wired network. As a result of identified weaknesses in this scheme, WEP was superseded by Wi-Fi Protected Access (WPA), and then by the full IEEE 802.11i standard (also known as WPA2).
- **WPA**
  - Wi-Fi Protected Access (WPA and WPA2) is a class of system used to secure wireless (Wi-Fi) computer networks. It was created in response to several serious weaknesses researchers had found in the previous WEP system. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared (WPA2).
  - WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points.
  - To resolve problems with WEP, the Wi-Fi Alliance released WPA (FIG. 115) which integrated **802.1x**, **TKIP** and **MIC**. Within the WPA specifications the RC4 cipher engine was maintained from WEP. RC4 is widely used in SSL (Secure Socket Layer) to protect internet traffic.

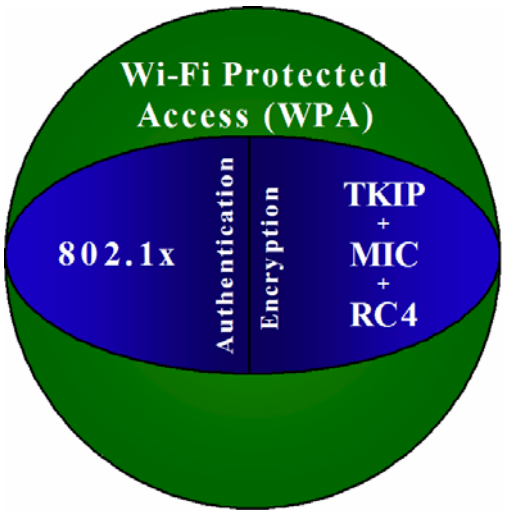


FIG. 115 WPA Overview

- **WPA2**
  - Also know as IEEE 802.11i, is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. The 802.11i scheme makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher.
  - The 802.11i architecture contains the following components: 802.1X for authentication (entailing the use of EAP and an authentication server), RSN for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication.
  - WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:
    - *either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.*
    - *in the "Personal" mode, the most likely choice for homes and small offices, a passphrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.*
  - With the RC4 released to the general public the IEEE implemented the Advanced Encryption Standard (AES) as the cipher engine for 802.11i, which the Wi-Fi Alliance has branded as WPA2.

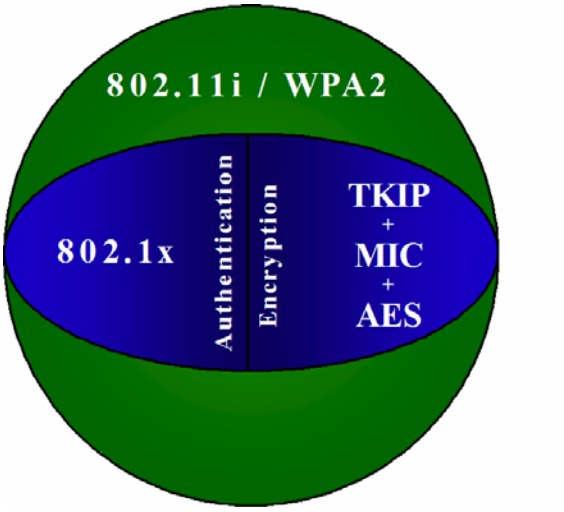


FIG. 116 WPA2 Overview

EAP Authentication

EAP (Extensible Authentication Protocol) is an Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. Although there are currently over 40 different EAP methods defined, the current internal Modero 802.11g wireless card and accompanying firmware only support the following EAP methods (***listed from simplest to most complex***):

- EAP-LEAP (Cisco Light EAP)
- EAP-FAST (Cisco Flexible Authentication via Secure Tunneling, a.k.a. LEAPv2)

The following use certificates:

- EAP-PEAP (Protected EAP)
- EAP-TTLS (Tunneled Transport Layer Security)
- **EAP-TLS** (Transport Layer Security)

EAP requires the use of an 802.1x authentication server (also known as a Radius server). Sophisticated Access Points (such as Cisco) can use a built-in Radius server. The most common RADIUS servers used in wireless networks today are:

- Microsoft Sever 2003
- Juniper Odyssey (once called Funk Odyssey)
- Meetinghouse AEGIS Server
- DeviceScape RADIUS Server
- Cisco Secure ACS

EAP characteristics

The following table outlines the differences among the various EAP Methods from most secure (at the top) to the least secure (at the bottom of the list):

EAP Method Characteristics				
Method:	Credential Type:	Authentication:	Pros:	Cons:
EAP-TLS	• Certificates	• Certificate is based on a two-way authentication	• Highest Security	• Difficult to deploy
EAP-TTLS	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Client authentication is done via password and certificates • Server authentication is done via certificates	• High Security	• Moderately difficult to deploy
EAP-PEAP	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Client authentication is done via password and certificates • Server authentication is done via certificates	• High Security	• Moderately difficult to deploy
EAP-LEAP	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Authentication is based on MS-CHAP and MS-CHAPv2 authentication protocols	• Easy deployment	• Susceptible to dictionary attacks
EAP-FAST	• Certificates • Fixed Passwords • One-time passwords (tokens)	• N/A	• N/A	• N/A

EAP communication overview

EAP Authentication goes a step beyond just encrypting data transfers, but also requires that a set of credentials be validated before the client (panel) is allowed to connect to the rest of the network (FIG. 117). Below is a description of this process. It is important to note that there is no user intervention necessary during this process. It proceeds automatically based on the configuration parameters entered into the panel.

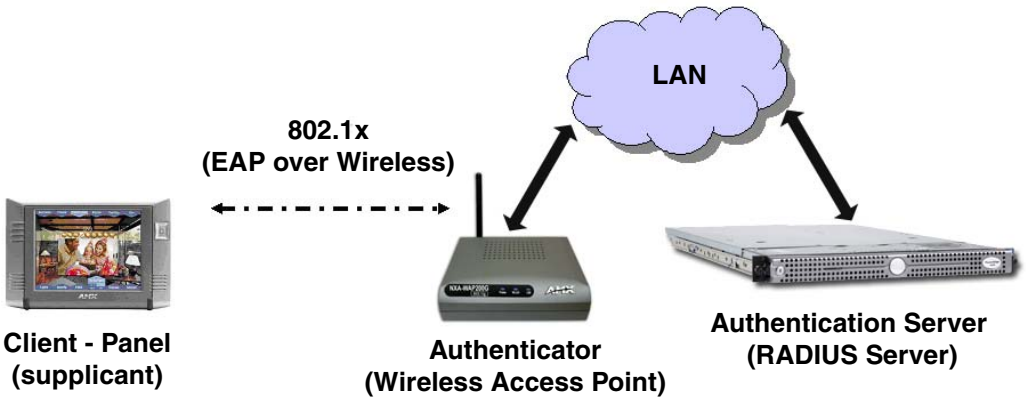


FIG. 117 EAP security method in process

1. The client (panel) establishes a wireless connection with the WAP specified by the SSID.
2. The WAP opens up a tunnel between itself and the RADIUS server configured via the access point. This tunnel means that packets can flow between the panel and the RADIUS server but nowhere else. ***The network is protected until authentication of the client (panel) is complete and the ID of the client is verified.***
3. The WAP (Authenticator) sends an "EAP-Request/Identity" message to the panel as soon as the wireless connection becomes active.
4. The panel then sends a "EAP-Response/Identity" message through the WAP to the RADIUS server providing its identity and specifying which EAP type it wants to use. If the server does not support the EAP type, then it sends a failure message back to the WAP which will then disconnect the panel. As an example, EAP-FAST is only supported by the Cisco server.
5. If the EAP type is supported, the server then sends a message back to the client (panel) indicating what information it needs. This can be as simple as a username (*Identity*) and password or as complex as multiple CA certificates.
6. The panel then responds with the requested information. If everything matches, and the panel provides the proper credentials, the RADIUS server then sends a success message to the access point instructing it to allow the panel to communicate with other devices on the network. At this point, the WAP completes the process for allowing LAN Access to the panel (possibly a restricted access based on attributes that came back from the RADIUS server).
    - As an example, the WAP might switch the panel to a particular VLAN or install a set of firewall rules.

AMX Certificate Upload Utility

The Certificate Upload utility gives you the ability to compile a list of target touch panels, select a pre-obtained certificate (uniquely identifying the panel), and then upload that file to the selected panel.

NOTE

This application must be run from a local machine and should not be used from a remote network location.

This application ensures that a unique certificate is securely uploaded to a specific touch panel. Currently, the target panels must be capable of supporting the WPA-PSK and EAP-XXX wireless security formats.

The Certificate Upload utility supports the following capabilities:

- Ability to browse both a local and network drive to find a desired certificate file.
- Ability to create a list of target AMX G4 touch panels based on IP Addresses
  - Compatible panels include: MVP-8400, MVP-7500, NXD-CV10, NXT-CV10, NXD-CV7, and NXT-CV7.
- Ability to display the IP Address of the local computer hosting the application.
- Ability to load a previously created list of target touch panels.
- Ability to save the current list of target Modero panel as a file.
- Ability to track the progress of the certificate upload by noting the current data size being transmitted and any associated error messages (if any).

The Certificate Upload Utility recognizes the following certificate file types:

- **CER** (Certificate File)
- **DER** (Distinguished Encoding Rules)
- **PEM** (Privacy Enhanced Mail)
- **PFX** (Normal Windows generated certificate)
- **PVK** (Private Key file)

Configuring your G4 Touch Panel for USB Communication

For a personal computer to establish a connection to a Modero panel via USB, the target computer must have the appropriate AMX USB driver installed. This installation is bundled into the latest TPDesign4 and NetLinx Studio2 software setup process or can be downloaded independently from the main Application Files page on www.amx.com.

NOTE

Close the Certificate Upload Utility before configuring the touch panel's USB driver. Only after the panel has been successfully setup to communicate via USB can you then re-launch the utility.

Step 1: Setup the Panel and PC for USB Communication

1. If you do not currently have the latest version of TPDesign4, navigate to **www.amx.com > Tech Center > Downloadable Files > Application Files > NetLinx Design Tools** section of the website and locate the AMX USB Driver executable (AMX USBLAN Setup exe).
2. Download this executable file to a known location on your computer.
3. Launch the Setup.exe and follow the on-screen prompts to complete the installation.

Step 2: Confirm the Installation of the USB Driver on the PC

The first time each AMX touch panel is connected to the PC it is detected as a new hardware device and the USBLAN driver becomes associated with it (panel specific). Each time thereafter the panel is "recognized" as a unique USBLAN device and the association to the driver is done in the background. When the panel is detected for the first time some user intervention is required during the association between panel and driver.

1. After the installation of the USB driver has been completed, confirm the proper installation of the large Type-A USB connector to the PC's USB port, and restart your machine.

If the panel is already powered, continue with steps 3. The panel MUST be powered and configured for USB communication before connecting the mini-USB connector to the panel's Program Port.

2. Connect the terminal end of the power cable to the 12 VDC power connector on the side/rear of the pane, and supply power. If using an MVP that is installed onto a docking station, feed power to the docked panel by connecting the appropriate power supply to the docking station.

3. After the panel powers-up, access the firmware setup pages by either:
   - **MVP** - Pressing and holding the two lower buttons on both sides of the display for 3 seconds.
   - **CV7/CV10** - Pressing the grey Front Setup Access button for 3 seconds.
4. Select Protected Setup > System Settings (located on the lower-left) to open the System Settings page.
5. Toggle the blue *Type* field (from the Master Connection section) until the choice cycles to **USB**.
   - The connection remains RED after changing the communication from Ethernet to USB until the panel is rebooted.
   - Once the panel restarts, the connection turns a dark green until connected to an active USB cable.
6. Press the **Back** button on the touch panel to return to the Protected Setup page.
7. Press the on-screen **Reboot** button to both save any changes and restart the panel. Remember that the panel's connection type must be set to USB prior to rebooting the panel and prior to inserting the USB connector.
8. **ONLY AFTER** the unit displays the first panel page, **THEN** insert the mini-USB connector into the Program Port on the panel.
   - It may take a minute for the panel to detect the new connection and send a signal to the PC (indicated by a green System Connection icon). If this is your first time installing the USB driver, a USB driver installation popup window appears on the PC.
9. Complete the USB driver installation process by clicking **Yes** and then installing the new AMX USB LAN LINK when told that a new USB device was found. This action accepts the installation of the new AMX USB driver.
10. Reboot the panel. Once restarted, the panel is now configured to communicate directly with the PC.

The mini-USB connector MUST be then plugged into an already active panel before the PC can recognize the connection and assign an appropriate USB driver. This driver is part of both the NetLinx Studio and TPDesign4 software application installations.

11. Launch the Certificate Upload Utility and confirm the utility has detected the new USB connection to the panel:
    - Click on the ***Local Address*** field's drop-down arrow.
    - Confirm the new USB entry shows up in the list as: **10.XX.XX.1**.

How to Upload a Certificate File

1. Install the latest AMX USB LAN LINK driver onto your computer by installing the latest versions of either TPDesign4 or NetLinx Studio2. This USB driver prepares your computer to properly communicate with a directly connected G4 touch panel (MVP/CV7/CV10).
    - Refer to Step 1 from within the previous *Step 1: Setup the Panel and PC for USB Communication* section on page 203.
2. Access the target panel's Protected Setup firmware page and configure the USB communication parameters.
    - Refer to Step 2 from within the previous *Step 2: Confirm the Installation of the USB Driver on the PC* section on page 204.
3. With the panel successfully communicating with target computer, launch the Certificate Upload Utility.
    - Familiarize yourself with the User Interface options (Certificate Utility User Interface).
4. Locate your certificate file by using the **Browse** button and navigating to the desired file type.
5. Use the drop-down arrow in the *Local Address* field to select communication through either the computer's Ethernet port (Internet communication) or via the USB port (direct connection). If using an Ethernet connection skip to step 8.
6. **For a USB connection**, select the ***10.XX.XX.1*** IP Address which corresponds to the virtual IP Address assigned to the USB connection port on the computer.
7. **For a USB connection**, navigate to the *Add IP Address* field (bottom-right of the interface) and enter a value of **1** greater than the virtual USB IP Address.
    - For example: If the virtual USB IP Address is **10.0.0.1** then you would add an address for the directly connected panel of **10.0.0.2** (this is one greater than the USB address value detected by the utility).
    - **You can send a certificate to ONLY ONE directly connected panel (via USB)**. If using the Ethernet port's IP Address, you can send a server certificate to multiple target panels.
8. **For an Ethernet IP Address connection**, select the IP Address which corresponds to the local computer's Ethernet address.
9. Navigate to the *Add IP Address* field (bottom-right of the interface) and enter the IP Addresses of the various target touch panels.
10. Click the **Add** button to complete the entry and add the new IP Address to the listing of available device IP Addresses. Repeat this process for all subsequent device IP Addresses.
11. Once your list is complete, click on the **File** drop-down menu and select the **Save** option to launch a Save dialog where you can assign a name to the current list of addresses and then save the information (as a TXT (text) file) to a known location.

This application must be run from a local machine and should not be used from a remote network location.

12. Select the target devices which be uploaded with the selected certificate. These can either be:
    - individually selected by toggling the box next to the Send entry (with the Type column).
    - selected as a group by clicking on the Check All radio box located at the top of the device IP Address listing.
13. When you are ready to send the certificate file to the selected panels, click the **Send** button to initiate the upload.
    - Once the *Status* field for each entry reads **Done**, your upload was successfully completed.

It's Your World - Take Control™

3000 RESEARCH DRIVE, RICHARDSON, TX 75082 USA • 800.222.0193 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support • www.amx.com

10/07 ©2007 AMX. All rights reserved. AMX and the AMX logo are registered trademarks of AMX. AMX reserves the right to alter specifications without notice at any time.